

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"JnanaSangama", Belgaum -590014, Karnataka.



LAB REPORT
on

Ethical Hacking

Submitted by

Rajdeep Bandyopadhyay (1BM22IC045)

in partial fulfillment for the award of the degree of
BACHELOR OF ENGINEERING

in
COMPUTER SCIENCE AND ENGINEERING(IoT and Cybersecurity including Blockchain)



B.M.S. COLLEGE OF ENGINEERING

(Autonomous Institution under VTU)

BENGALURU-560019

March-2025 to June-2025



Edit with WPS Office

B. M. S. College of Engineering,

Bull Temple Road, Bangalore 560019

(Affiliated To Visvesvaraya Technological University, Belgaum)

Department of Computer Science and Engineering(IoT and Cybersecurity including Blockchain)



CERTIFICATE

This is to certify that the Lab work entitled “Ethical Hacking” carried out by **Rajdeep Bandyopadhyaya (1BM22IC045)**, who is a bonafide student of B. M. S. College of Engineering. It is in partial fulfillment for the award of Bachelor of Engineering in Computer Science and Engineering(IoT and Cybersecurity including Blockchain) of the Visvesvaraya Technological University, Belgaum during the year 2025. The Lab report has been approved as it satisfies the academic requirements in respect of a Ethical Hacking (23IC6PCEHG) work prescribed for the said degree.

Krupa K S
Assistant Professor
Department of CSE(ICB)
BMSCE, Bengaluru

Dr. Prasad G R
Professor and Head
Department of CSE(ICB)
BMSCE, Bengaluru



Edit with WPS Office

Index Sheet

| Sl. No. | Experiment Title | Page No. |
|---------|---|----------|
| 1 | Ethical Hacking Fundamentals | 1-28 |
| 2 | Information Security Threats and Vulnerability Assessment | 29-45 |
| 3 | Password Cracking Techniques and Countermeasures | 46-61 |
| 4 | Social Engineering Techniques and Countermeasures | 62-73 |
| 5 | Network Level Attack and Countermeasures | 74-100 |
| 6 | Web Application Attack and Countermeasures | 101-133 |
| 7 | Wireless Attack and Countermeasures | 134-137 |
| 8 | Mobile Attack and Countermeasures | 138-161 |
| 9 | IOT and OT Attack and Countermeasures | 162-178 |
| 10 | Cloud Computing Threats and Countermeasures | 179-186 |



Edit with WPS Office

Ethical Hacking Report – 01 (Date: 22-03-2025)

Ethical Hacking Fundamentals

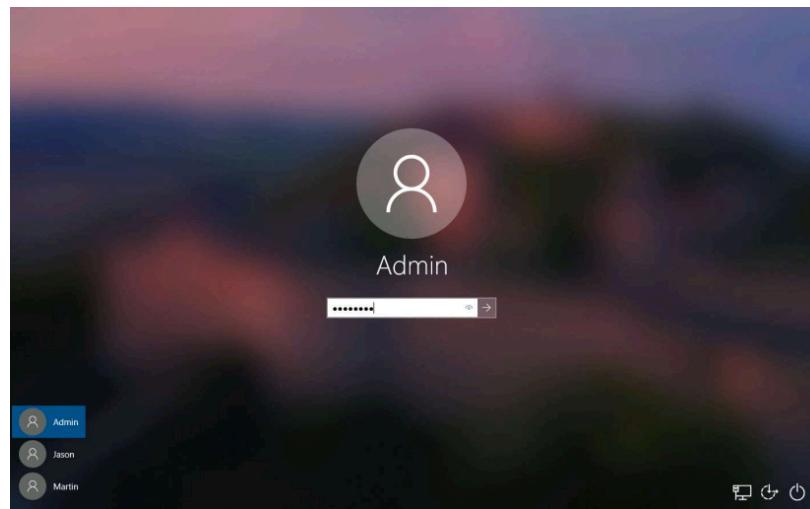
EC-Council Lab Assignment: Module 2

Perform passive footprinting to gather information about a target

Ethical hackers or pen testers use numerous tools and techniques to collect information about the target. Here we learned various footprinting techniques include:

1. Gather information using advanced google hacking technique

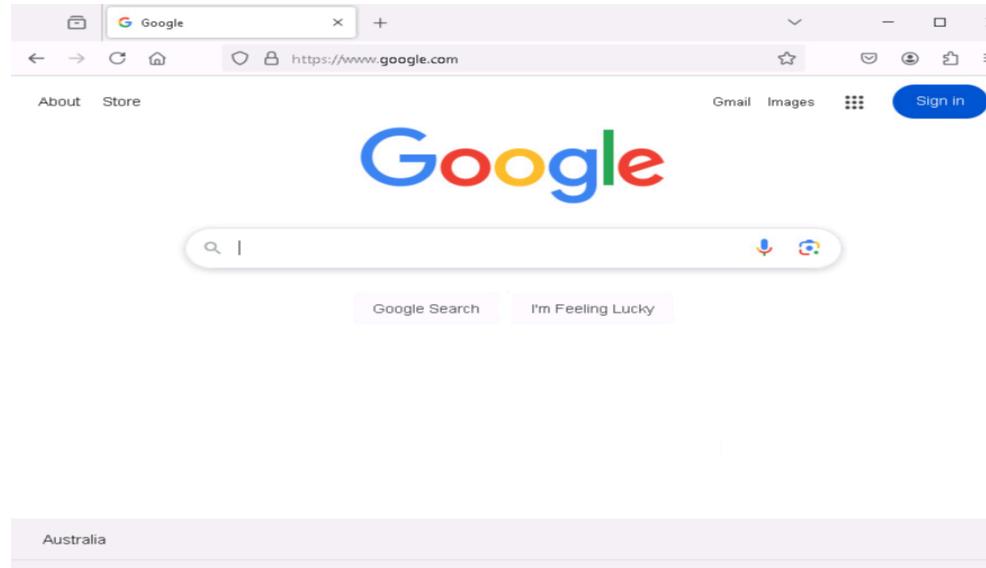
- 1.1. First select the Windows 10 machine and press **Ctrl+Alt+Delete** (or use the button in the Resources pane or Commands menu).
- 1.2. Click **Pa\$\$w0rd** to paste it in the Password field and press **Enter** to log in.



- 1.3. If the **Welcome to Windows** wizard appears, click **Continue**, then click **Cancel** in the **Sign in with Microsoft** wizard.
- 1.4. On the **Networks** screen, click **Yes** to allow network discovery.
- 1.5. Open **Mozilla Firefox**, type <https://www.google.com> in the address bar, and press **Enter**.



Edit with WPS Office



1.6. If a **Default Browser** pop-up appears, uncheck the checkbox and click **Not now**.

1.7. If a **Content Blocking** pop-up appears, click **Got it**.

1.8. If a **notification** appears at the top, click **Okay, Got it**, then click **I agree** in the Google Search wizard.

1.9. When Google search appears, dismiss any pop-ups by clicking **No, thanks**.

1.10. Use filter **intitle:hacking site:www.eccouncil.org** in a search command
The query will show results only from the **EC-Council** website where the word "hacking" appears in the title.

intitle:hacking site:www.eccouncil.org

All Images Videos News Short videos Shopping Forums More Tools

EC-Council
https://www.eccouncil.org › cybersecurity-exchange

What is Ethical Hacking
Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit an ...

EC-Council
https://www.eccouncil.org › Train & Certify

CEH Certification | Ethical Hacking Training & Course
20 learning modules covering over 550 attack techniques, CEH provides you with the core knowledge you need to thrive as a cybersecurity professional.

EC-Council
https://www.eccouncil.org › ethical-hacking › system-h...

What is System Hacking? Definition, Types and Processes
28 Mar 2023 — System hacking refers to using technical skills and knowledge to gain access to a computer system or network.

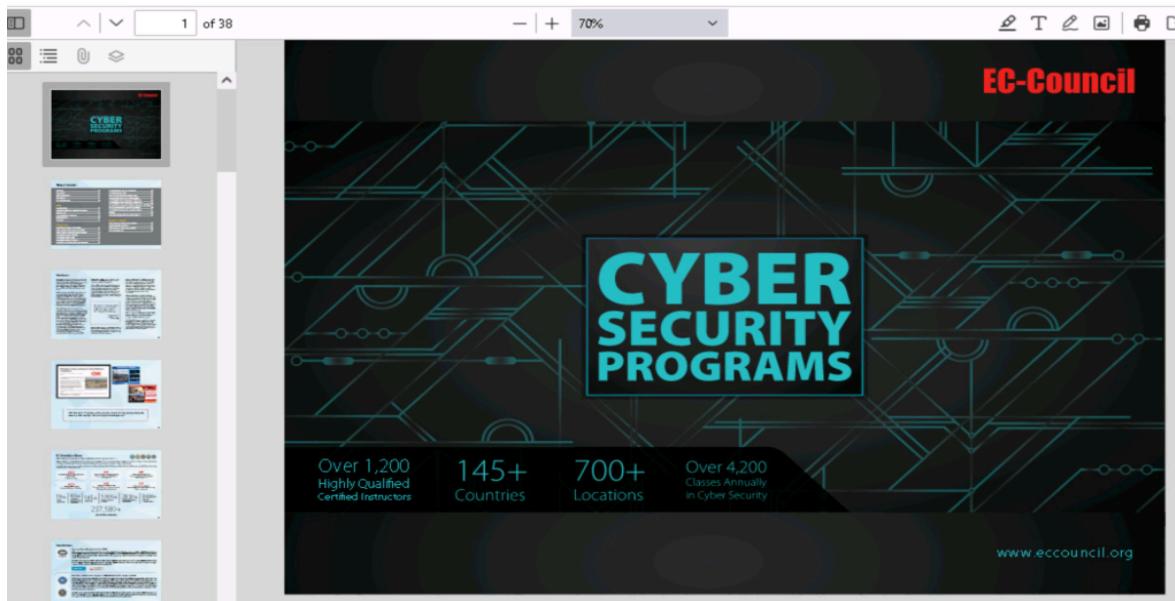


Edit with WPS Office

- 1.11. Use the filter **EC-Council filetype:pdf** is a search command. The query will show PDF files related to EC-Council in the search results.

A screenshot of a Google search results page. The search query is "Ec-Council filetype:pdf". The top result is a PDF file titled "Cyber-Handbook-Enterprise-2.2.pdf" from the EC-Council website. The snippet shows that EC-Council creates content and certification delivered through authorized training centers, with 38 pages. Below the result, there is a "People also ask" section with four expandable questions: "What is the EC-Council?", "What is the EC-Council controversy?", "Which is better CompTIA or EC-Council?", and "Is EC-Council free?".

- 1.12. Now, click on any link from the results



This will appear displaying the PDF file, as shown in the screenshot.



Edit with WPS Office

- 1.13. In the search bar, type the command **allinurl: ethical hacking** and press **Enter** to search your results containing the word specified in the URL.

The screenshot shows a Google search results page with the query "allinurl: ethical hacking". The results are as follows:

- EC-Council** - https://www.eccouncil.org/cybersecurity-exchange
- What is Ethical Hacking** - Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit...
- Black Duck** - https://www.blackduck.com/glossary/what-is-ethical...
- What Is Ethical Hacking and How Does It Work?** - Ethical hacking is an authorized attempt to gain unauthorized access to a computer system, application, or data using the strategies and actions of...
- IBM** - https://www.ibm.com/think/topics/ethical-hacking
- What is Ethical Hacking? | IBM** - 20 Oct 2023 — Ethical hacking is the use of hacking techniques by friendly parties in an attempt to uncover, understand and fix security vulnerabilities ...
- Infosecurity Europe** - https://www.infosecurityeurope.com/guides-checklists
- What is Ethical Hacking and How Does It Work?**

On the right side of the screenshot, there is a sidebar with instructions and screenshots:

- 13. The page displays only pages containing the words "ethical" and "hacking" in the URL, as shown in the screenshot.
- 14. Now, click back icon present on the top-left corner of the browser window to navigate back to <https://www.google.com>.

At the bottom right, there are navigation buttons for "Previous" and "Next", and a timer showing "59 Minutes Remaining".

The page displays only pages containing the words “ethical” and “hacking” in the URL, as shown in the screenshot.

- 1.14. Now go back and filter **related:www.eccouncil.org** is a search command used in search engines.

The query will show websites that are similar or related to EC-Council's website.



Edit with WPS Office

Instructions

15. In the search bar, type the command related:www.eccouncil.org and press Enter to search your results that are similar or related to the URL specified.

16. The page displays Google search engine results page with websites similar to eccouncil.org, as shown in the screenshot.

Resources

Previous Next 54 Minutes Remaining

17. Apart from the aforementioned advanced Google operators, you can also use the following to perform an advanced search to gather more information about the target organization from publicly available sources.
- cache: This operator allows you to view cached version of the web page. [cache:www.google.com]—Query returns the cached version of the website www.google.com
 - inurl: This operator restricts the results to pages containing the word specified in the URL [inurl: copy site:www.google.com]—Query returns only pages in Google site in which the URL has the word "copy"
 - allintitle: This operator restricts results to pages containing all the query terms specified in the title. [allintitle: detect malware]—Query returns only pages containing the words "detect" and "malware" in the title
 - inanchor: This operator restricts results to pages containing the query terms specified in the anchor text on links to the page. [Anti-virus inanchor:Norton]—Query returns only pages with anchor text on links to the pages containing the word "Norton" and the page containing the word "Anti-virus"
 - allinanchor: This operator restricts results to pages containing all query terms specified in the anchor text on links to the page. [allinanchor: best cloud service provider]—Query returns only pages in which the anchor text on links to the pages contain the words "best," "cloud," "service," and "provider"
 - link: This operator searches websites or pages that contain links to the specified website or page. [link:www.googleguide.com]—Finds pages that point to Google Guide's home page
 - info: This operator finds information for the specified web page. [info:gohotel.com]—Query provides information about the national hotel directory GotHotel.com home page
 - location: This operator finds information for a specific location. [location: 4 seasons restaurant]—Query give you results based around the term 4 seasons restaurant
18. This concludes the demonstration of gathering information using advanced Google hacking techniques. You can conduct a series of queries on your own by using these advanced Google operators and gather the relevant information about the target organization.
19. Close all open windows and document all the acquired information.

Question 2.1.1.1

Use an advanced Google hacking technique to find PDF files on the www.eccouncil.org website. Enter the complete URL of the Cyber-Handbook-Enterprise-2.pdf file.

Score

✓ Correct

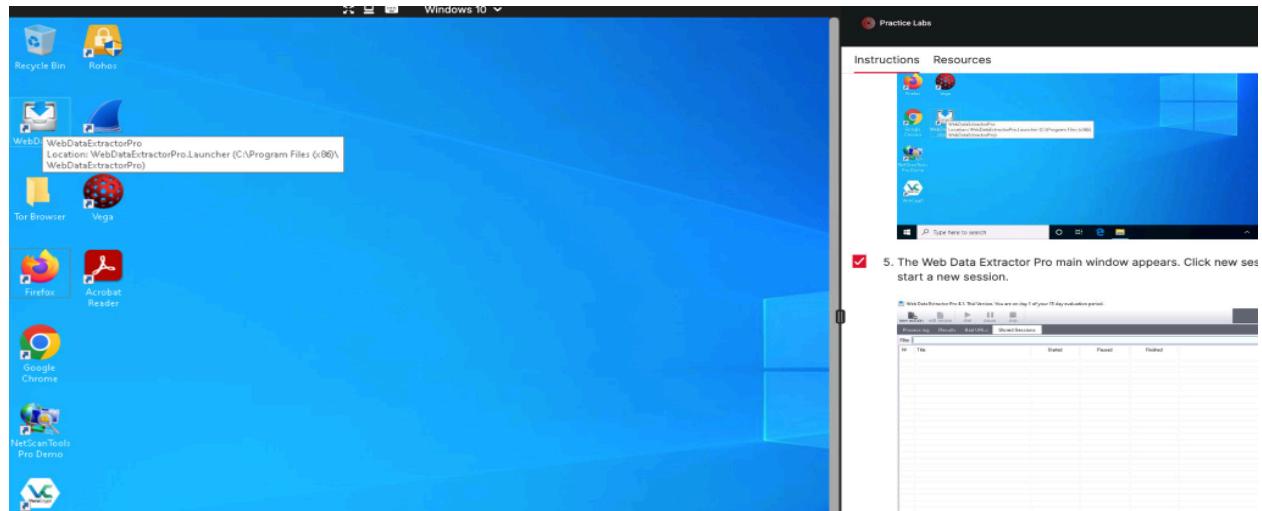


Edit with WPS Office

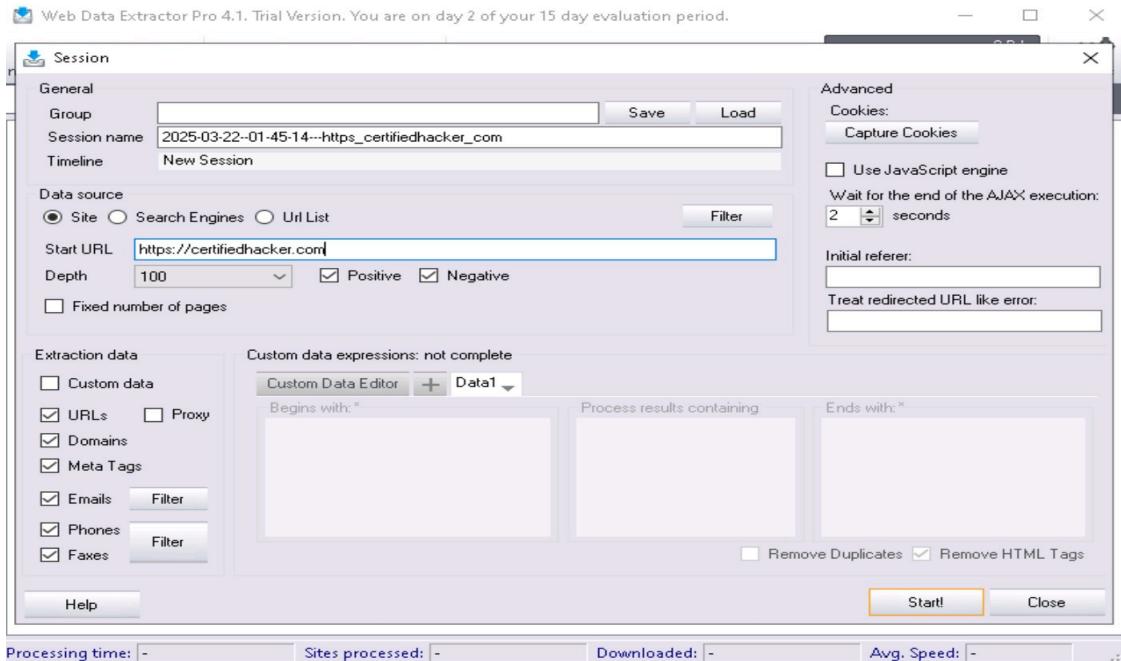
2. Extract a company's data using Web Data Extractor

Web data extraction gathers information from a company's website, including contact details, URLs, and meta tags. Tools like **Web Data Extractor** use web spiders to automate data collection for ethical hacking.

- 2.1. Follow the wizard steps to install Web Data Extractor Pro and click **Finish**.
- 2.2. After installation, launch **Web Data Extractor Pro** from Desktop.



- 2.3. Launch The **Web Data Extractor Pro** main window appears. Click **new session** to start a new session.



Edit with WPS Office

The Session window appears; type a URL (here, <https://www.certifiedhacker.com>) in the **Start URL** field. Check all the options, as shown in the screenshot and Click **Start** to initiate the data extraction.

2.4. Now click on **Results** tab to view the collected information about the website.

The screenshot shows the Web Data Extractor Pro interface. At the top, it says "Web Data Extractor Pro 4.1. Trial Version. You are on day 2 of your 15 day evaluation period." Below the title bar are buttons for "new session", "edit session", "start", "pause", and "stop". To the right is a graph showing "0 B/s" and an "options" gear icon. The main window has tabs at the top: "Process log", ***Results**, "Bad URLs (11)", and "Stored Sessions". The "*Results" tab is selected, showing a table with 20 rows of extracted meta-tag data. The columns are "Description", "Keywords", "Title", "Url", and "Host". Below the table, status information includes "Processing time: 00:00:15.151", "Sites processed: 62 / 78", "Downloaded: 796 KB", and "Avq. Speed: 214 KB/s".

| Description | Keywords | Title | Url | Host |
|-----------------------------------|------------------------------------|----------------------------------|--|---------------------|
| A brief description of this we... | keywords, or phrases, asso... | Certified Hacker | https://certifiedhacker.com/ | certifiedhacker.com |
| Professional Real Estate Se... | real estate, real estate listin... | Professional Real Estate S... | https://certifiedhacker.com/Real%20... | certifiedhacker.com |
| A short description of your c... | Some keywords that best d... | Your company - Homepage | https://certifiedhacker.com/Recipes/... | certifiedhacker.com |
| | | Clear Construction | https://certifiedhacker.com/corporate... | certifiedhacker.com |
| | | P-Folio | https://certifiedhacker.com/P-folio/in... | certifiedhacker.com |
| | | Under The Trees | https://certifiedhacker.com/Under%20... | certifiedhacker.com |
| Turbo max powerful one pa... | Turbo max , owltemplates.c... | Turbo Max Theme - OwlTe... | https://certifiedhacker.com/Turbo%20... | certifiedhacker.com |
| A brief description of this we... | keywords, or phrases, asso... | Unite - Together is Better [...] | https://certifiedhacker.com/Social%20... | certifiedhacker.com |
| Online Booking | booking, hotel, hotels, rese... | Online Booking | https://certifiedhacker.com/Online%20... | certifiedhacker.com |
| A short description of your c... | Some keywords that best d... | Your company - Recipes d... | https://certifiedhacker.com/Recipes/... | certifiedhacker.com |
| A short description of your c... | Some keywords that best d... | Your company - Menu | https://certifiedhacker.com/Recipes/... | certifiedhacker.com |
| A short description of your c... | Some keywords that best d... | Your company - About us | https://certifiedhacker.com/Recipes/... | certifiedhacker.com |
| A short description of your c... | Some keywords that best d... | Your company - Recipes | https://certifiedhacker.com/Recipes/... | certifiedhacker.com |
| A short description of your c... | Some keywords that best d... | Your company - Contact us | https://certifiedhacker.com/Recipes/... | certifiedhacker.com |
| Online Booking | booking, hotel, hotels, rese... | Online Booking: Sitemap | https://certifiedhacker.com/Online%20... | certifiedhacker.com |
| Online Booking | booking, hotel, hotels, rese... | Online Booking: Browse D... | https://certifiedhacker.com/Online%20... | certifiedhacker.com |
| Online Booking | booking, hotel, hotels, rese... | Online Booking: FAQ | https://certifiedhacker.com/Online%20... | certifiedhacker.com |
| Online Booking | booking, hotel, hotels, rese... | Online Booking: Typography | https://certifiedhacker.com/Online%20... | certifiedhacker.com |
| A short description of your c... | Some keywords that best d... | Your company - Recipes c... | https://certifiedhacker.com/Recipes/... | certifiedhacker.com |

- Select the **Meta tag** tab to view details like URL, Title, Keywords, and Description.
- Select the **Email** tab to see email-related information.
- Select the **Phone** tab to check phone details.
- Explore the **Fax, Link, and Domain** tabs for more information.

2.5. This completes the demonstration of Web Data Extractor Pro for extracting company data.

Question 2.1.2.1

In the Windows 10 machine, use Web Data Extractor Pro web spidering tool located at D:\EHE-Tools\EHE Module 02 Ethical Hacking Fundamentals\Web Spiders\Web Data Extractor to gather the target company's data. Enter the target website that was used in this task to gather information.

Score

Correct



Edit with WPS Office

3. Perform whois lookup using DomainTools

Whois is a protocol used to query databases storing details of domain owners and IP addresses. It operates on port 43 (TCP) and is managed by Regional Internet Registries (RIRs). Whois databases provide information such as owner details, creation & expiration dates. DomainTools can be used to perform a Whois lookup to gather target information.

- 3.1. On the Windows 10 machine, open a web browser (**Mozilla Firefox**). In the address bar, enter <http://whois.domaintools.com> and press **Enter** to open the Whois Lookup website



- 3.2. Enter a domain or IP address... search bar, type www.certifiedhacker.com and click Search.



Edit with WPS Office

DomainTools PROFILE ▾ CONNECT ▾ MONITOR ▾ SUPPORT WHOIS ▾

LOG IN Sign Up

Home > Whois Lookup > CertifiedHacker.com

Notice: Possible deprecation of Whois services after January 28, 2025. [More Info ↗](#)

Whois Record for CertifiedHacker.com

Domain Profile

| | |
|------------------|---|
| Registrar | Network Solutions, LLC IANA ID: 2 URL: http://networksolutions.com Whois Server: whois.networksolutions.com domain.operations@web.com (p) +18777228662 |
| Registrar Status | clientTransferProhibited |
| Dates | 8,270 days old Created on 2002-07-30 Expires on 2025-07-30 Updated on 2024-08-22 |
| Name Servers | NS1.BLUEHOST.COM (has 2,051,267 domains) NS2.BLUEHOST.COM (has 2,051,267 domains) |
| IP Address | 162.241.216.11 - 920 other sites hosted on this server |
| IP Location | USA - Utah - Provo - Unified Layer |
| ASN | AS46606 UNIFIEDLAYER-AS-1, US (registered Oct 24, 2008) |

DomainTools Iris
The gold-standard internet intelligence platform [Learn More](#)

Tools

- Hosting History
- Monitor Domain Properties
- Reverse IP Address Lookup
- Network Tools
- Visit Website

Preview the Full Domain Report

View Screenshot History

Available TLDs

DomainTools PROFILE ▾ CONNECT ▾ MONITOR ▾ SUPPORT WHOIS ▾

LOG IN Sign Up

Domain Status Registered And No Website

IP History 13 changes on 13 unique IP addresses over 19 years

Hosting History 2 changes on 3 unique name servers over 10 years

Whois Record (last updated on 2025-03-22)

Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376.DOMAIN.COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: <http://networksolutions.com>
Updated Date: 2024-08-22T07:51:37Z
Creation Date: 2002-07-30T00:32:00Z
Registrar Registration Expiration Date: 2025-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32256
Registrant Country: US
Registrant Phone: +1.5707086622
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: kq9t994x73e@networksolutionsprivateregistration.com
Registrant Admin ID:

General TLDs Country TLDs

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

- Taken domain.
- Available domain.
- Deleted previously owned domain.

| | |
|----------------------|----------------------------|
| CertifiedHacker.com | View Whois |
| CertifiedHacker.net | View Whois |
| CertifiedHacker.org | View Whois |
| CertifiedHacker.info | Buy Domain |
| CertifiedHacker.biz | Buy Domain |
| CertifiedHacker.us | Buy Domain |

This concludes the demonstration of gathering target organization information using Whois lookup on DomainTools.



Edit with WPS Office

Question 2.1.3.1

Perform Whois Lookup using DomainTools (<http://whois.domaintools.com>) and find the Registrant Postal Code of www.certifiedhacker.com website.

32256

Score

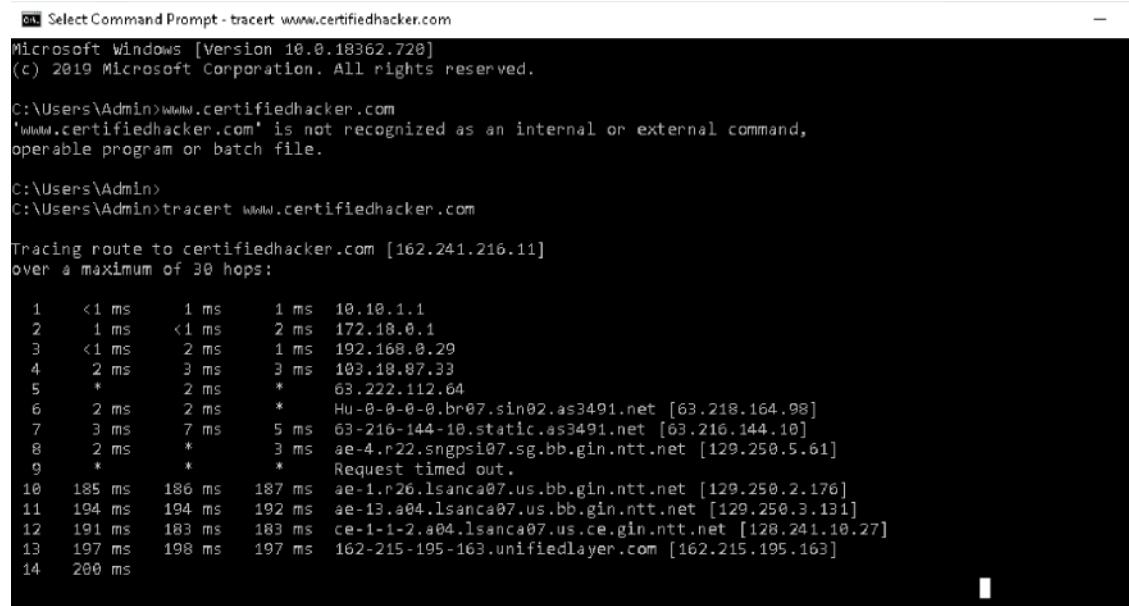
✓ Correct

2. Perform network scanning to identify live hosts, open ports and services and target OS in the network

o Perform network tracerouteing in Windows and Linux machines

Network tracerouting identifies the path a packet takes between the source and destination. It provides details like **IP addresses of intermediate hosts**, helping map **network topology**. Traceroute reveals **trusted routers, firewall locations, and network structure** of an organization.

- open the **Command Prompt** window. Type **tracert www.certifiedhacker.com** and press **Enter** to view the hops that the packets made before reaching the destination



```
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Admin>www.certifiedhacker.com
'www.certifiedhacker.com' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Admin>
C:\Users\Admin>tracert www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

 1  <1 ms    1 ms    1 ms  10.18.1.1
 2  1 ms    <1 ms    2 ms  172.18.0.1
 3  <1 ms    2 ms    1 ms  192.168.0.29
 4  2 ms    3 ms    3 ms  103.18.87.33
 5  *        2 ms    *   68.222.112.64
 6  2 ms    2 ms    *   Hu-0-0-0-0.br07.sin02.as3491.net [63.218.164.98]
 7  3 ms    7 ms    5 ms  63-216-144-10.static.as3491.net [63.216.144.10]
 8  2 ms    *        3 ms  ae-4.r22.sngpsi07.sg.bb.gin.ntt.net [129.250.5.61]
 9  *        *        *   Request timed out.
10  185 ms   186 ms   187 ms  ae-1.r26.lsanca07.us.bb.gin.ntt.net [129.250.2.176]
11  194 ms   194 ms   192 ms  ae-13.a04.lsanca07.us.bb.gin.ntt.net [129.250.3.131]
12  191 ms   183 ms   183 ms  ce-1-1-2.a04.lsanca07.us.ce.gin.ntt.net [128.241.10.27]
13  197 ms   198 ms   197 ms  162-215-195-163.unifiedlayer.com [162.215.195.163]
14  200 ms


```

- Type **tracert /?** and press **Enter** to show the different options for the command, as shown in the screenshot.



Edit with WPS Office

```
Command Prompt
16  205 ms  204 ms  204 ms  69-195-64-111.unifiedlayer.com [69.195.64.111]
17  194 ms  195 ms  195 ms  po97.prv-leafia.net.unifiedlayer.com [162.144.240.123]
18  198 ms  198 ms  198 ms  box5331.bluehost.com [162.241.216.11]

Trace complete.

C:\Users\Admin>
C:\Users\Admin>
C:\Users\Admin>
C:\Users\Admin>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
                [-R] [-S srcaddr] [-4] [-6] target_name

Options:
  -d           Do not resolve addresses to hostnames.
  -h maximum_hops   Maximum number of hops to search for target.
  -j host-list     Loose source route along host-list (IPv4-only).
  -w timeout       Wait timeout milliseconds for each reply.
  -R           Trace round-trip path (IPv6-only).
  -S srcaddr      Source address to use (IPv6-only).
  -4           Force using IPv4.
  -6           Force using IPv6.

C:\Users\Admin>
```

- Type **tracert -h 5 www.certifiedhacker.com** and press **Enter** to perform the trace, but with only 5 maximum hops allowed.

```
Command Prompt
[-R] [-S srcaddr] [-4] [-6] target_name

Options:
  -d           Do not resolve addresses to hostnames.
  -h maximum_hops   Maximum number of hops to search for target.
  -j host-list     Loose source route along host-list (IPv4-only).
  -w timeout       Wait timeout milliseconds for each reply.
  -R           Trace round-trip path (IPv6-only).
  -S srcaddr      Source address to use (IPv6-only).
  -4           Force using IPv4.
  -6           Force using IPv6.

C:\Users\Admin>tracert -h 5 www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 5 hops:

  1  <1 ms    <1 ms    1 ms  10.10.1.1
  2  <1 ms    <1 ms    1 ms  172.18.0.1
  3  <1 ms    <1 ms    <1 ms  192.168.0.29
  4  2 ms     1 ms    2 ms  103.18.87.33
  5  2 ms     4 ms    2 ms  63.222.112.64

Trace complete.

C:\Users\Admin>
```

- The results are displayed, as shown in the screenshot.



Edit with WPS Office

```

C:\ Command Prompt

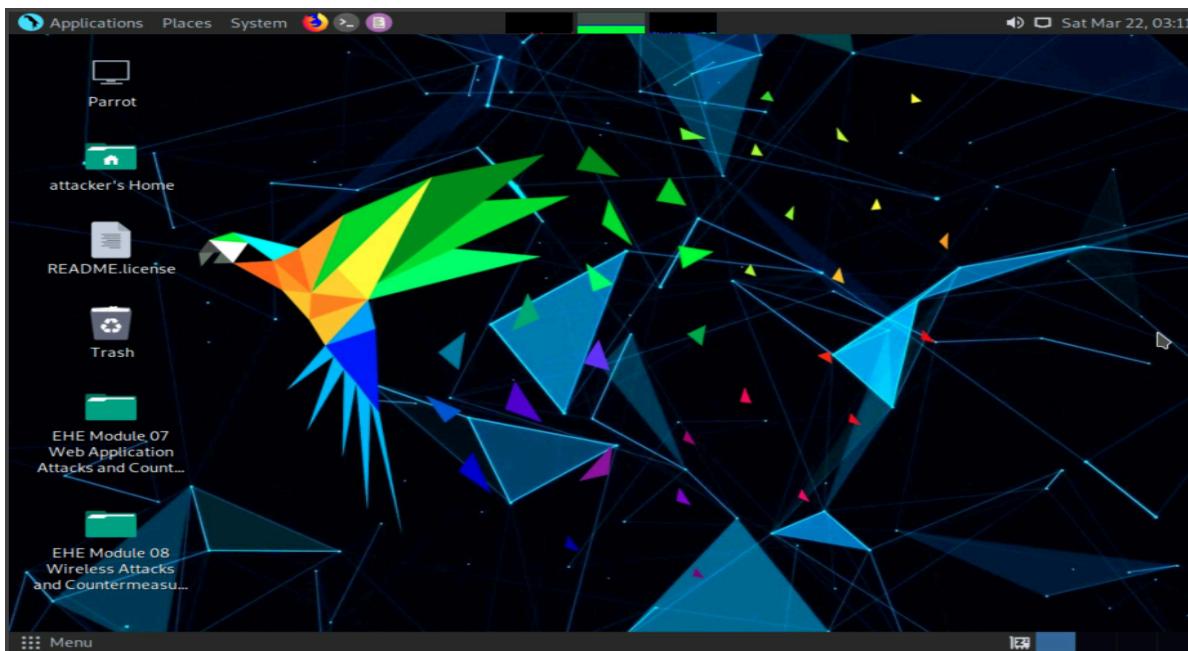
C:\Users\Admin>tracert -w 5 www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

 1  2 ms    <1 ms      1 ms  10.10.1.1
 2  1 ms    <1 ms      <1 ms  172.18.0.1
 3  <1 ms    <1 ms      <1 ms  192.168.0.29
 4  2 ms    1 ms      1 ms  103.18.87.33
 5  2 ms    2 ms      2 ms  63.222.112.64
 6  *        *         3 ms  Hu-0-0-0-0.br07.sin02.as3491.net [63.218.164.98]
 7  *        1 ms      1 ms  63-216-144-10.static.as3491.net [63.216.144.10]
 8  *        3 ms      *     ae-4.r22.sngpsi07.sg.bb.gin.ntt.net [129.250.5.61]
 9  84 ms    *         100 ms ae-4.r27.osakjp02.jp.bb.gin.ntt.net [129.250.2.67]
10  187 ms   185 ms    *     ae-1.r26.lsanca07.us.bb.gin.ntt.net [129.250.2.176]
11  193 ms   193 ms    *     ae-13.a04.lsanca07.us.bb.gin.ntt.net [129.250.3.131]
12  179 ms   179 ms    *     ce-1-1-2.a04.lsanca07.us.ce.gin.ntt.net [128.241.10.27]
13  197 ms   198 ms    *     162-215-195-163.unifiedlayer.com [162.215.195.163]
14  201 ms   *         203 ms 162-215-193-229.unifiedlayer.com [162.215.193.229]
15  208 ms   208 ms    *     69-195-64-235.unifiedlayer.com [69.195.64.235]
16  204 ms   204 ms    *     69-195-64-111.unifiedlayer.com [69.195.64.111]
17  194 ms   194 ms    *     po97.prv-leafia.net.unifiedlayer.com [162.144.240.123]
18  198 ms   198 ms    *     box5331.bluehost.com [162.241.216.11]
19  198 ms   199 ms    *     box5331.bluehost.com [162.241.216.11]
20  198 ms   198 ms    *     box5331.bluehost.com [162.241.216.11]
21  198 ms   198 ms    *     box5331.bluehost.com [162.241.216.11]
22  198 ms   199 ms    *     box5331.bluehost.com [162.241.216.11]
23  198 ms   199 ms    *     box5331.bluehost.com [162.241.216.11]
24  199 ms   198 ms    *     box5331.bluehost.com [162.241.216.11]

```

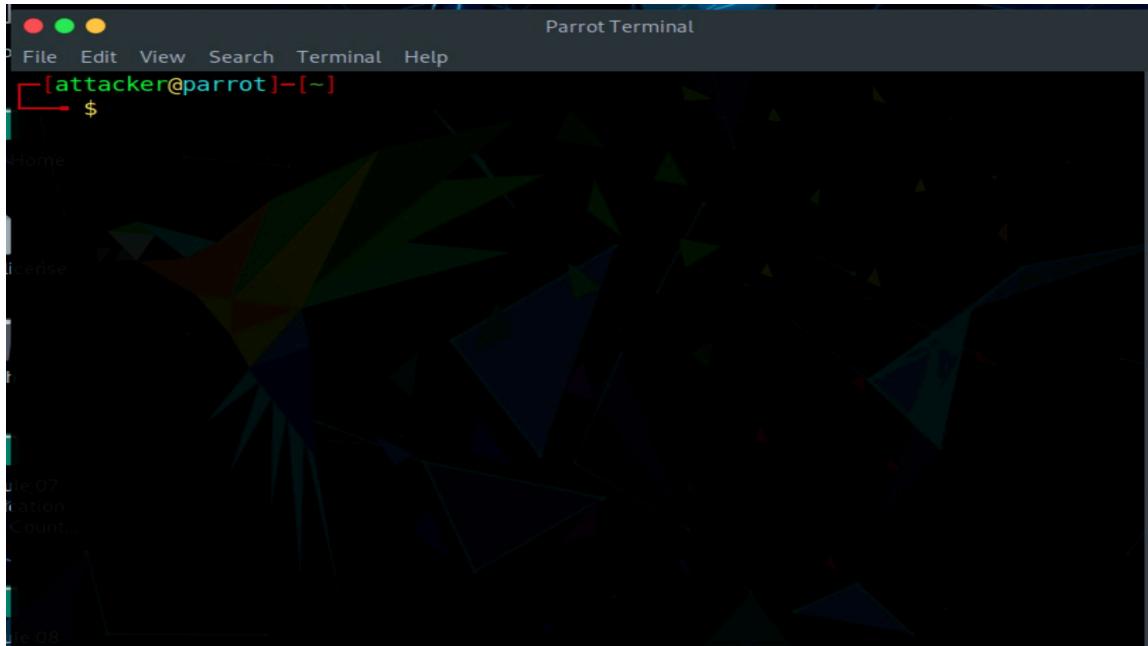
- Now performing same using Parrot Security 4.10



- Open MATE Terminal icon at the top-left corner of the Desktop window to open a Terminal window.



Edit with WPS Office



- in the terminal window, type **traceroute** www.certifiedhacker.com and enter

```
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot] - [~]
$traceroute www.certifiedhacker.com
traceroute to www.certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte packets
 1  10.10.1.1 (10.10.1.1)  0.163 ms  0.142 ms  0.126 ms
 2  172.18.0.1 (172.18.0.1)  0.267 ms  0.252 ms  0.236 ms
 3  192.168.0.29 (192.168.0.29)  0.531 ms  0.516 ms  0.499 ms
 4  * 103.18.87.33 (103.18.87.33)  1.956 ms *
 5  63.222.112.64 (63.222.112.64)  2.209 ms *
 6  Hu-0-0-0-0.br07.sin02.as3491.net (63.218.164.98)  29.747 ms Hu-0-0-0-2.br07.sin02.
.as3491.net (63.218.164.102)  26.265 ms  26.248 ms
 7  63-216-144-10.static.as3491.net (63.216.144.10)  2.780 ms  3.248 ms  3.225 ms
 8  * * ae-4.r22.sngpsi07.sg.bb.gin.ntt.net (129.250.5.61)  15.978 ms
 9  ae-2.r23.sngpsi07.sg.bb.gin.ntt.net (129.250.4.74)  18.064 ms ae-4.r27.osakjp02.j
.p.bb.gin.ntt.net (129.250.2.67)  84.394 ms *
10  ae-1.r26.lsanca07.us.bb.gin.ntt.net (129.250.2.176)  212.022 ms  197.702 ms  197.
687 ms
11  ae-13.a04.lsanca07.us.bb.gin.ntt.net (129.250.3.131)  192.667 ms  206.164 ms  210.
006 ms
12  ce-1-1-2.a04.lsanca07.us.ce.gin.ntt.net (128.241.10.27)  199.511 ms  196.289 ms
199.479 ms
13  ae-13.a04.lsanca07.us.bb.gin.ntt.net (129.250.3.131)  179.210 ms  162-215-195-163.
unifiedlayer.com (162.215.195.163)  199.448 ms  209.100 ms
14  162-215-193-229.unifiedlayer.com (162.215.193.229)  233.513 ms  162-215-193-235.un
ifiedlayer.com (162.215.193.235)  216.416 ms ce-1-1-2.a04.lsanca07.us.ce.gin.ntt.net
```

The terminal window shows the output of the traceroute command. It lists 14 routers along the path to the destination. Each router entry includes its IP address or name, the number of the hop, and the round-trip time (RTT) in milliseconds for three consecutive packets. The RTT values fluctuate significantly, indicating network latency and bandwidth issues.

- Now, type **traceroute -m 5 www.certifiedhacker.com** and press **Enter** to set the max number of hops as **5** for the packet to reach the destination.



Edit with WPS Office

```
[└→ $traceroute -m 5 www.certifiedhacker.com
traceroute to www.certifiedhacker.com (162.241.216.11), 5 hops max, 60 byte packets
1 10.10.1.1 (10.10.1.1) 0.505 ms 0.479 ms 0.462 ms
2 172.18.0.1 (172.18.0.1) 0.578 ms 0.563 ms 0.547 ms
3 192.168.0.29 (192.168.0.29) 0.616 ms 0.601 ms 0.586 ms
4 103.18.87.33 (103.18.87.33) 2.024 ms 6.688 ms 6.739 ms
5 63.222.112.64 (63.222.112.64) 2.415 ms 2.399 ms 2.385 ms
[attacker@parrot]~$
```

- This concludes the demonstration of performing network tracerouting using the Windows and Linux machines.

Question 2.2.1.1

Perform network tracerouting using traceroute command in Linux machine for www.certifiedhacker.com domain. Enter the IP address of the target domain.

162.241.216.11

Score

✓ Correct

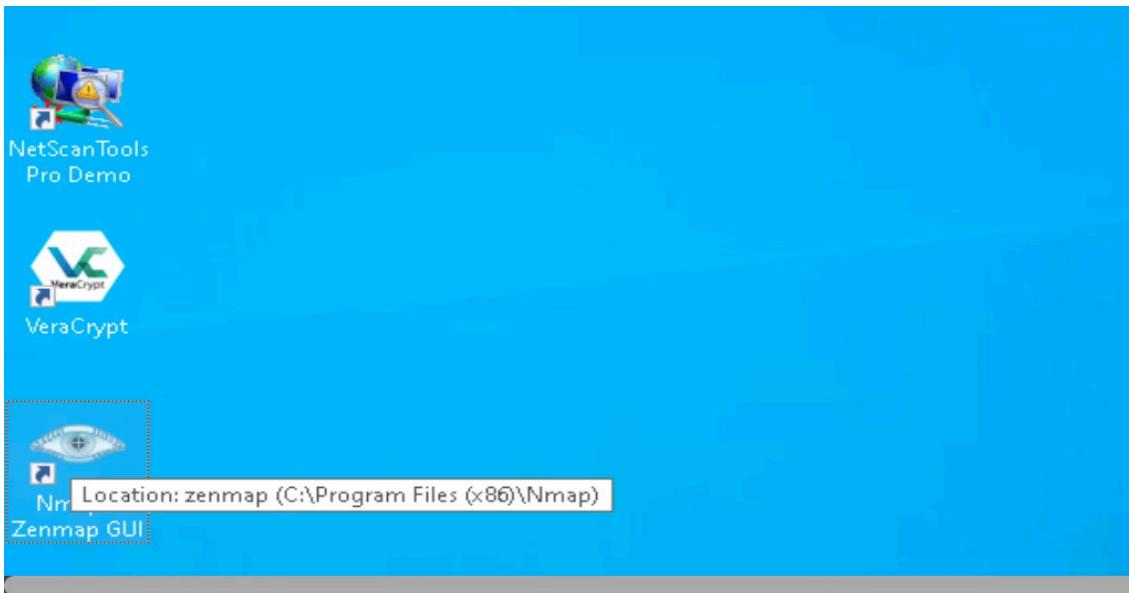
○ Perform host discovery using Nmap

Nmap is a tool for **network discovery, administration, and security auditing**. It helps with **network inventory, service monitoring, and uptime tracking**. Nmap can scan live hosts in a target network using techniques like ARP ping scan, UDP ping scan, and ICMP ECHO ping scan.

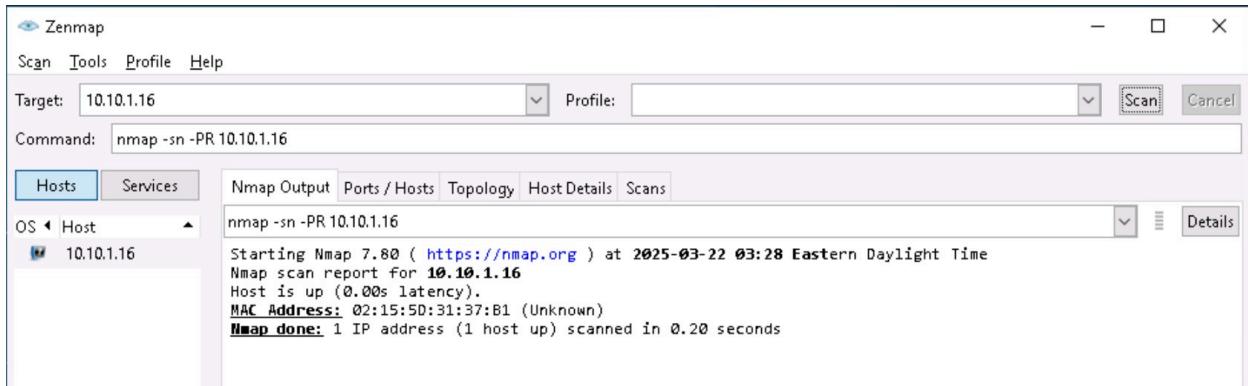
- Click on window 10 to switch to window 10.
- Navigate to the Desktop and double-click **Nmap - Zenmap GUI**



Edit with WPS Office



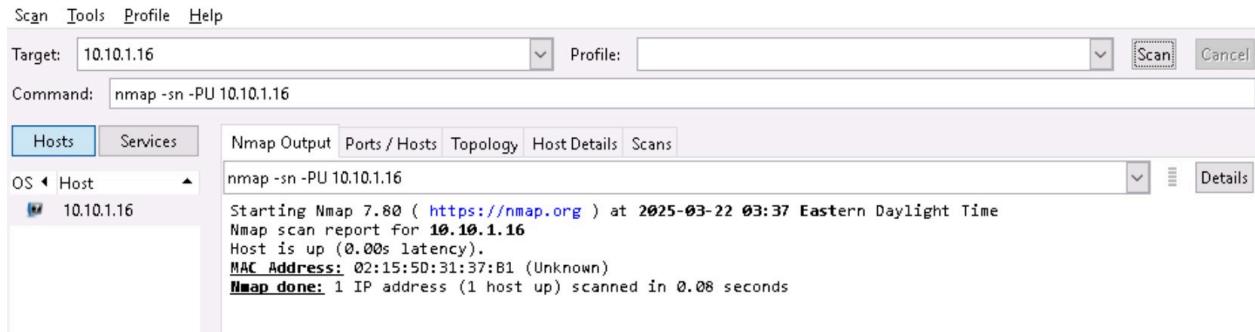
- In the **Command** field, type **nmap -sn -PR [Target IP Address]** (e.g., **10.10.1.16**) and click **Scan**.
- **-sn**: Disables port scanning.
- **-PR**: Performs an **ARP ping scan**.
- The scan results will confirm if the **target Windows Server 2016 (10.10.1.16)** host is **active**. • An **ARP request** is sent, and an **ARP response** indicates the host is **up**.



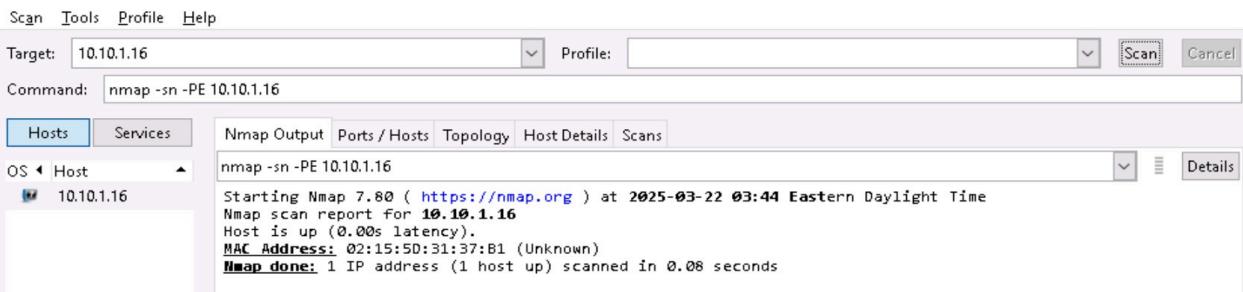
- In the **Command** field, type **nmap -sn -PU [Target IP Address]** (e.g., **10.10.1.16**) and click **Scan**.
- **-PU**: Performs a **UDP ping scan**.
- The scan sends **UDP packets** to the target. A **UDP response** confirms the host is **active**.
- If the host is **offline** or **unreachable**, error messages like "**host/network unreachable**" or "**TTL exceeded**" may appear.



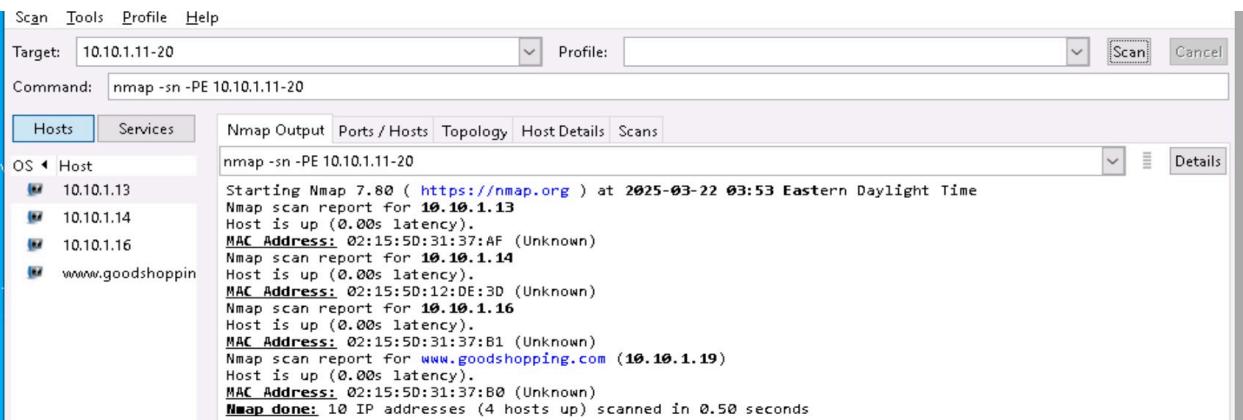
Edit with WPS Office



- To perform an ICMP ECHO ping scan, type **nmap -sn -PE [Target IP Address]** (e.g., **10.10.1.16**) in the Command field and click Scan.
- The results will indicate if the target host is up.
- PE: Executes an ICMP ECHO ping scan.

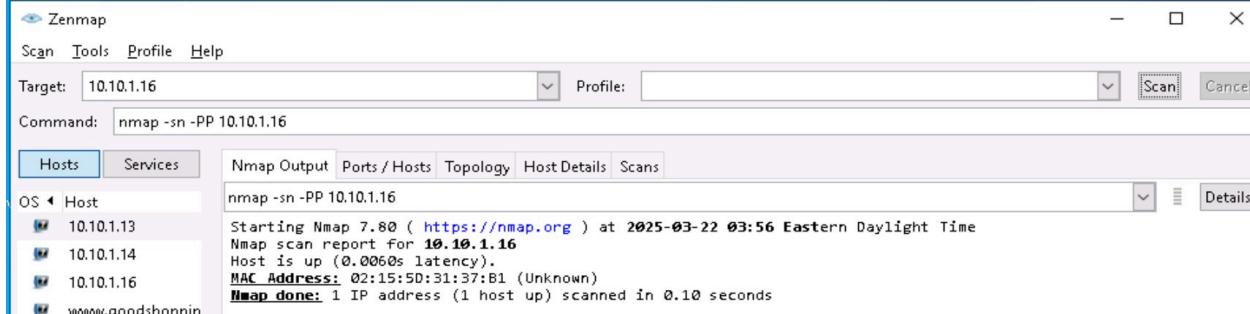


- In the Command field, type **nmap -sn -PE [Target Range of IP Addresses]** (e.g., **10.10.1.11-20**) and click Scan.
- PE: Performs an ICMP ECHO ping sweep.
- This scan sends ICMP ECHO requests to multiple hosts to identify live hosts. If a host is active, it replies with an ICMP ECHO response.

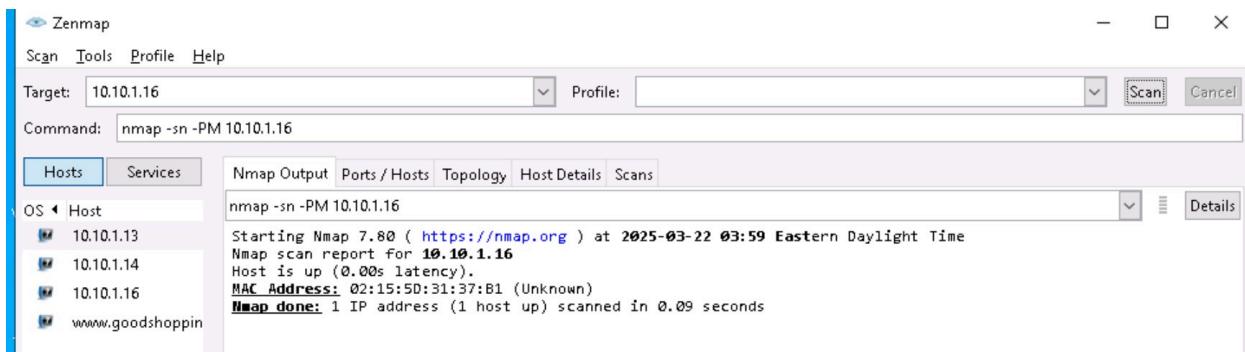


Edit with WPS Office

- In the Command field, type **nmap -sn -PP [Target IP Address]** (e.g., **10.10.1.16**) and click Scan.
 - **-PP:** Performs an ICMP timestamp ping scan.
- This scan sends ICMP timestamp requests to the target. If the target is active, it responds with a **timestamp reply**, providing information about the system's current time.



- In the Command field, type **nmap -sn -PM [Target IP Address]** (e.g., **10.10.1.16**) and click Scan.
- **-PM:** Performs an ICMP address mask ping scan.
- This scan sends an ICMP address mask query to the target to retrieve subnet mask information. It helps identify **active hosts**, especially when ICMP Echo requests are blocked by the administrator.



- Other techniques are:
 - **PM:** Performs the ICMP address mask ping scan.
 - **PP:** Performs the ICMP timestamp ping scan.
 - **TCP SYN Ping Scan:** Sends empty TCP SYN packets to the target host; an ACK response means that the host is active.
nmap -sn -PS [target IP address]
 - **TCP ACK Ping Scan:** Sends empty TCP ACK packets to the target host; an RST response means that the host is active.
nmap -sn -PA [target IP address]
 - **IP Protocol Ping Scan:** Sends probe packets of different IP protocols to the target host; any response indicates that a host is active. **nmap -sn -PO [target IP address]**



Edit with WPS Office

Question 2.2.2.1

Perform host discovery using Nmap and find the IP address of the machine hosting www.goodshopping.com.

10.10.1.19

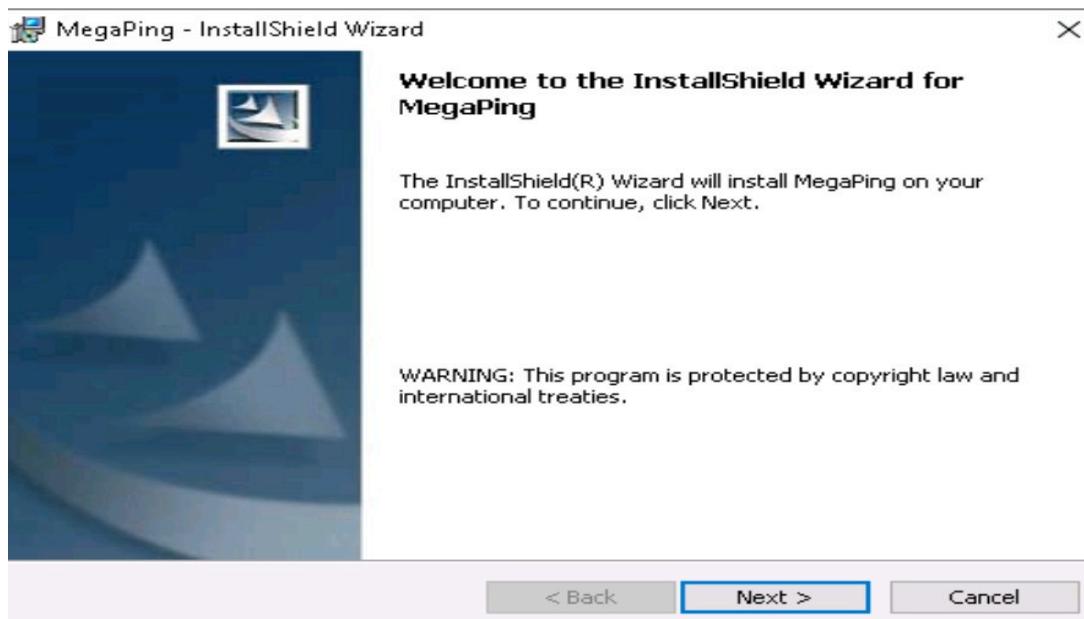
Score

✓ Correct

○ Perform port and service discovery using MegaPing

MegaPing is a powerful toolkit designed for IT professionals, system administrators, and security experts. It helps detect live hosts, scan open ports, and gather detailed system and network information. MegaPing can scan an entire network and provide details on shared resources, active services, registry entries, users, groups, trusted domains, and printers. Additionally, it includes network troubleshooting tools such as DNS lookup, IP and NetBIOS scanning, ping, port scanning, traceroute, and Whois.

- InstallShield Wizard window appears; click Next and follow the wizard-driven installation steps to install **MegaPing**.
- After the completion of the installation, click on the **Launch the program**



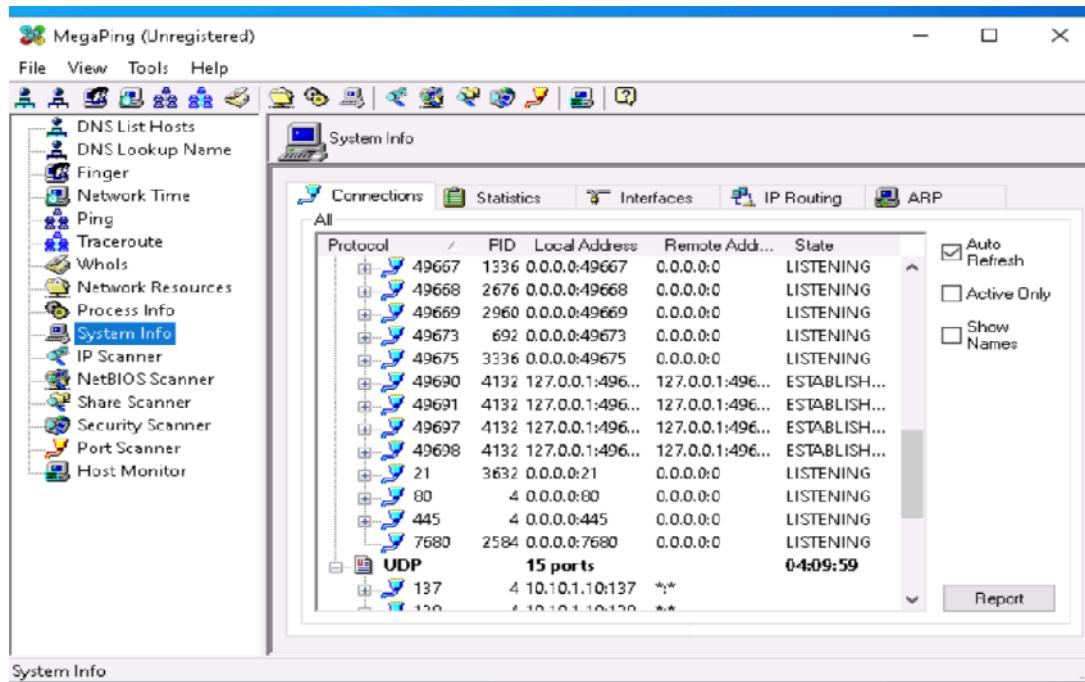
- The About MegaPing window appears; click the I Agree button.



Edit with WPS Office

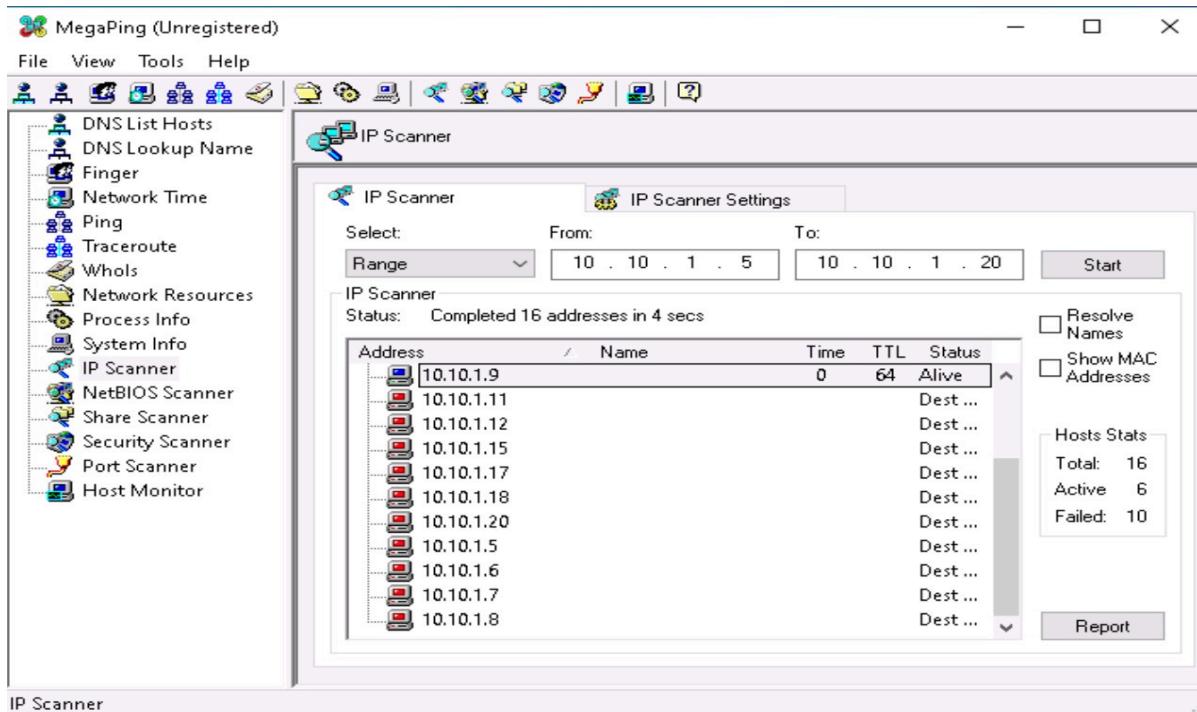


- The MegaPing (Unregistered) GUI appears displaying the System Info

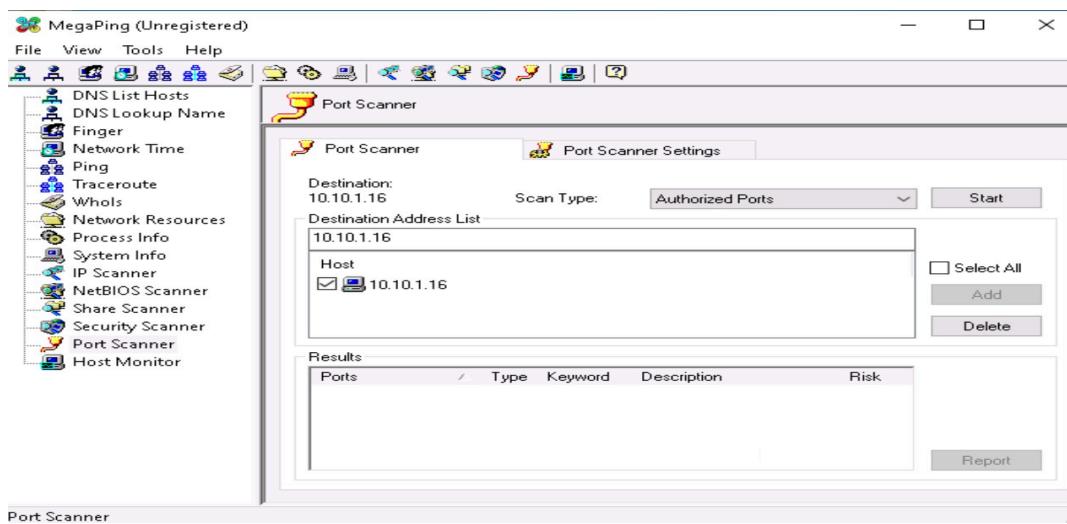


Edit with WPS Office

- Select the **IP Scanner** option from the left pane. In the **IP Scanner** tab on the right-hand pane, enter the IP range in the **From** and **To** fields. In this lab, the IP range is **10.10.1.5** to **10.10.1.20**. Then, click **Start** to begin the scanning process.
- MegaPing displays all IP addresses within the specified target range, along with their **TTL value**, **Status** (dead or alive), and statistics of the dead and alive hosts, as shown in the screenshot.

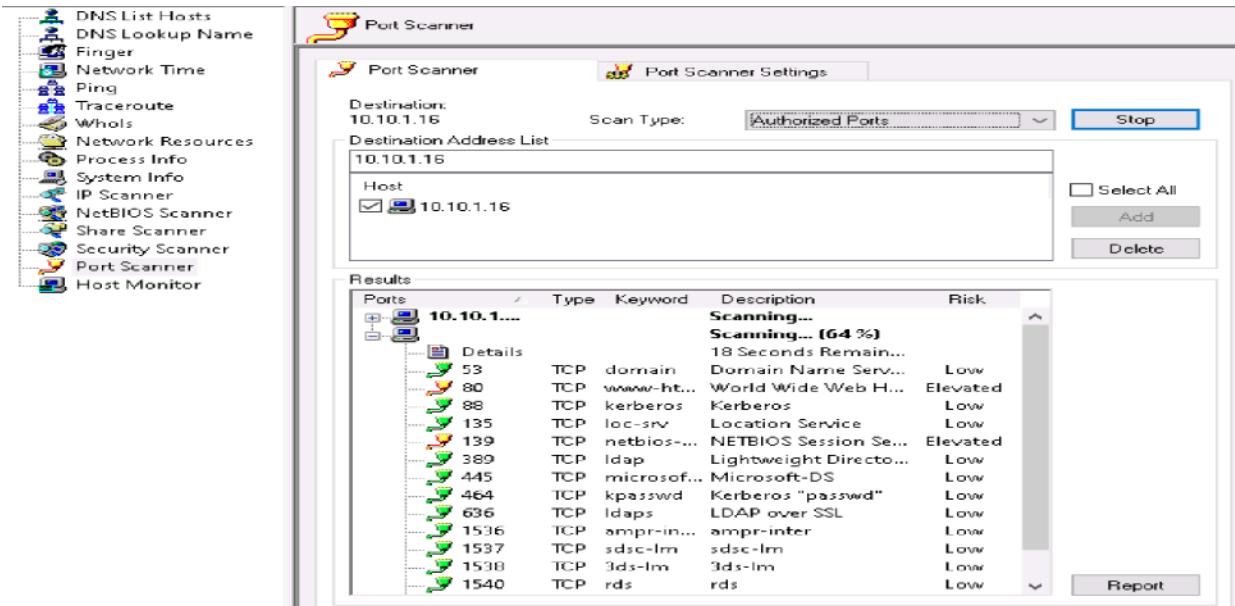


- Select the **Port Scanner** option from the left-hand pane. In the **Port Scanner** tab on the right, enter the **IP address of the Windows Server 2016 (10.10.1.16)** machine into the **Destination Address List** field and click **Add**.

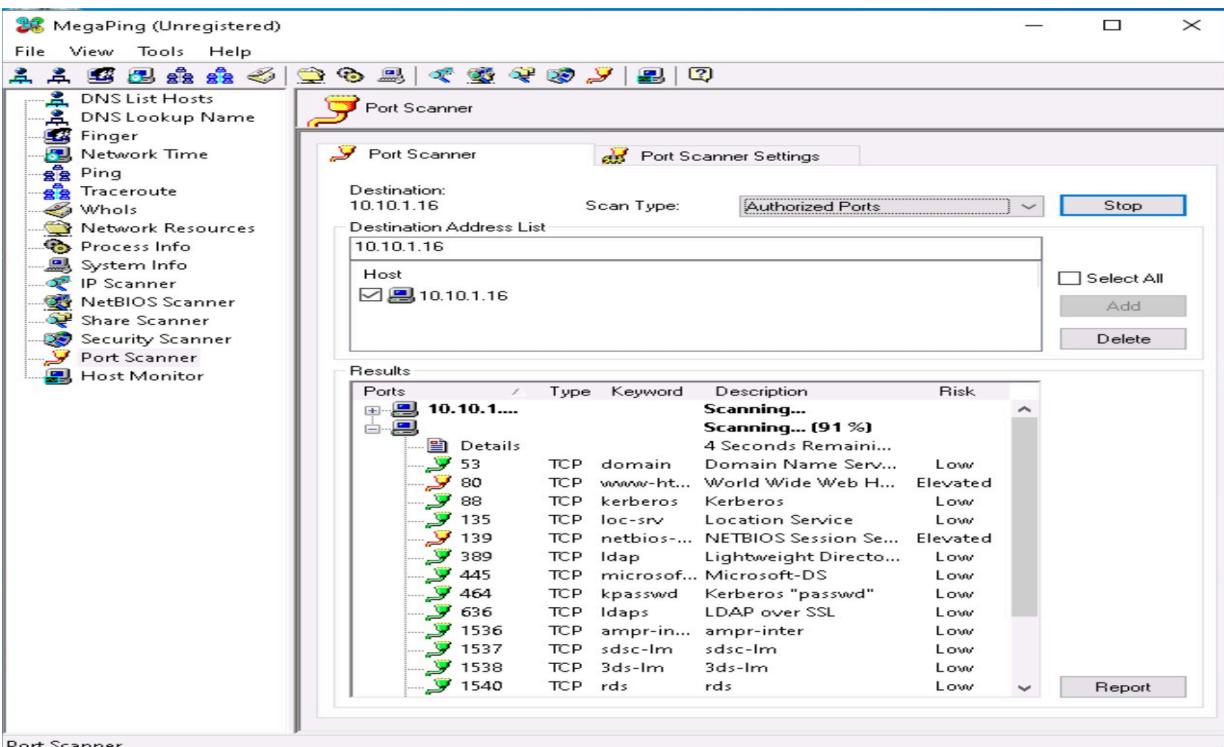


Edit with WPS Office

- Select the 10.10.1.16 checkbox and click the Start button to start listening to the traffic on 10.10.1.16.



- MegaPing displays the ports associated with Windows Server 2016 (10.10.1.16), providing details such as the port number and type, the service running on the port, a description of the service, and the associated risk, as shown in the screenshot.



Edit with WPS Office

Question 2.2.3.1

Perform port and service discovery using MegaPing available at Z:\EHE Module 02 Ethical Hacking Fundamentals\Scanning Tools\MegaPing and name the service running on port 389 on Windows Server 2016 machine.

Ldap

Score

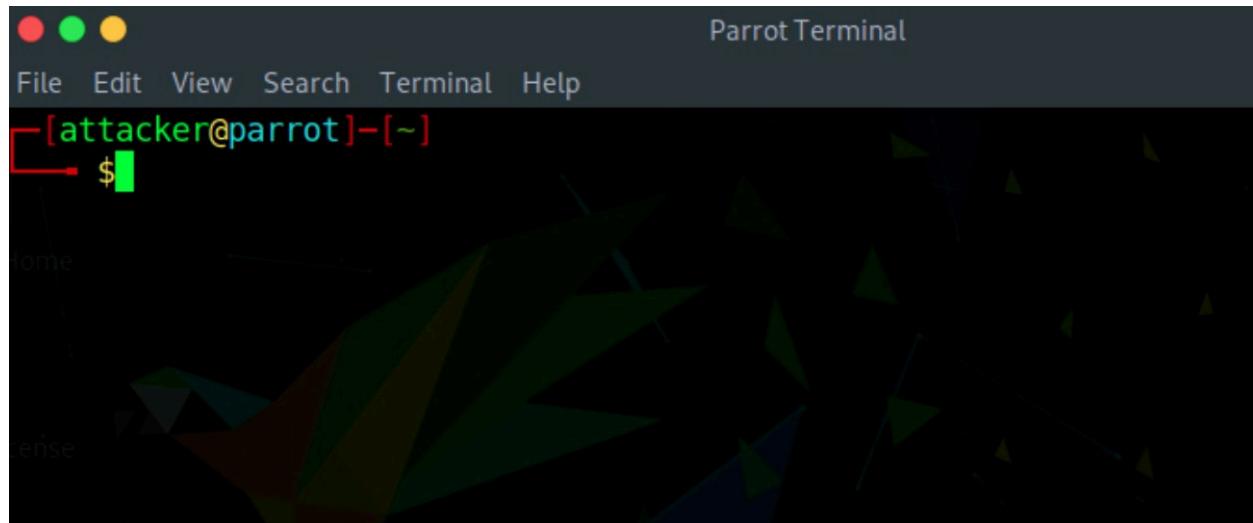
✓ Correct

○ Perform OS discovery using Unicornscan

Unicornscan is a Linux-based command-line tool for network reconnaissance and information gathering. It is an asynchronous TCP and UDP port scanner and banner grabber used to discover open ports, services, TTL values, and more on a target machine. By analyzing TTL values in the scan results, Unicornscan can help identify the operating system of the target machine.

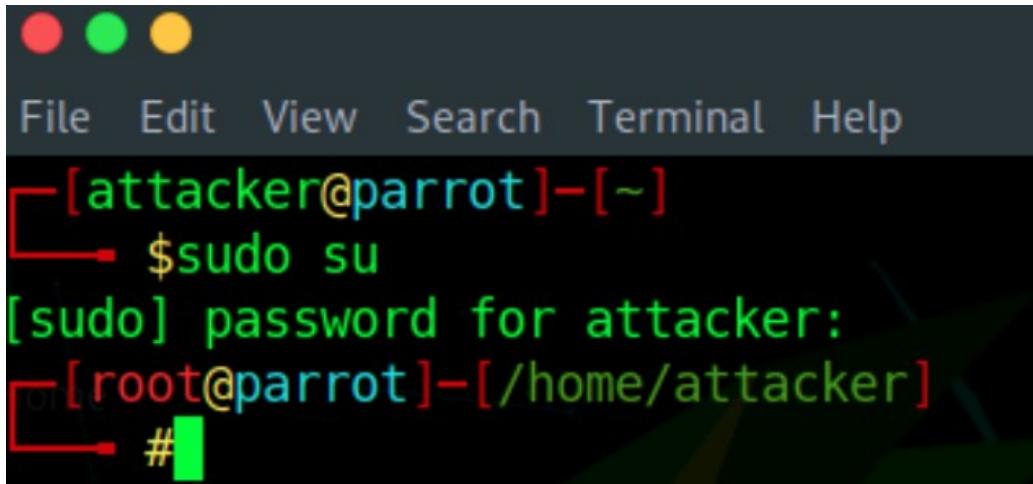
In this task, Unicornscan will be used to perform OS discovery on the target system.

- switch to the **Parrot Security** machine.
- Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window. •
Open the Parrot Terminal



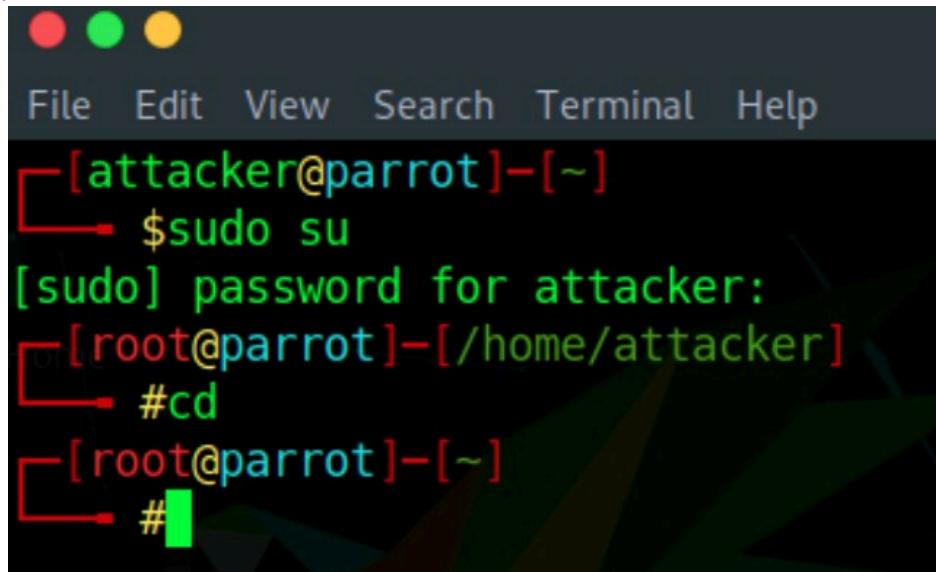
Edit with WPS Office

- Switch to Root User:
 - Type: sudo su and press enter
 - Enter Password:
 - In [sudo] password for attacker: field, type: toor
 - Press Enter
- (Note: The password will not be visible while typing.)



A terminal window titled "File Edit View Search Terminal Help". The prompt shows "[attacker@parrot]-(~)". The user types "\$sudo su" and hits enter. A message "[sudo] password for attacker:" appears. The user then types "toor" and hits enter. The prompt changes to "[root@parrot]-[/home/attacker]" and the hash symbol "#" is displayed at the end of the line.

- Navigate to the Root Directory:
 - Type: cd and Press Enter



A terminal window titled "File Edit View Search Terminal Help". The prompt shows "[attacker@parrot]-(~)". The user types "\$sudo su" and hits enter. A message "[sudo] password for attacker:" appears. The user then types "toor" and hits enter. The prompt changes to "[root@parrot]-[/home/attacker]" and the hash symbol "#" is displayed at the end of the line. The user then types "#cd" and hits enter. The prompt changes to "[root@parrot]-(~)" and the hash symbol "#" is displayed at the end of the line.



Edit with WPS Office

- Now, you are in the root environment and ready to execute **Unicornscan** commands.

```
[attacker@parrot]~
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
└─# cd
[root@parrot]~
└─# unicornscan 10.10.1.16
TCP open      domain[  53]      from 10.10.1.16 ttl 128
TCP open      http[   80]      from 10.10.1.16 ttl 128
TCP open      kerberos[  88]    from 10.10.1.16 ttl 128
TCP open      epmap[ 135]     from 10.10.1.16 ttl 128
TCP open      netbios-ssn[ 139]  from 10.10.1.16 ttl 128
TCP open      ldap[ 389]      from 10.10.1.16 ttl 128
TCP open      microsoft-ds[ 445] from 10.10.1.16 ttl 128
TCP open      ldaps[ 636]     from 10.10.1.16 ttl 128
TCP open      zephyr-clt[ 2103] from 10.10.1.16 ttl 128
TCP open      ms-wbt-server[ 3389]from 10.10.1.16 ttl 128
[root@parrot]~
└─# unicornscan 10.10.1.16 -Iv
adding 10.10.1.16/32 mode `TCPscan' ports `7,9,11,13,18,19,21-23,25,37,39,42,49,
50,53,65,67-70,79-81,88,98,100,105-107,109-111,113,118,119,123,129,135,137-139,1
43,150,161-164,174,177-179,191,199-202,204,206,209,210,213,220,345,346,347,369-3
72,389,406,407,422,443-445,487,500,512-514,517,518,520,525,533,538,548,554,563,5
37,610-612,631-634,636,642,653,655,657,666,706,750-752,765,779,808,873,901,923,9
```

- The command **unicornscan 10.10.1.16 -lv** is used to perform a detailed scan on the target machine, which in this case is a **Windows Server 2016** with the IP address **10.10.1.16**.
- unicornscan** → Runs Unicornscan, a network reconnaissance tool.
- 10.10.1.16** → Specifies the target IP address.
- l** → Enables **immediate mode** for faster scanning.
- v** → Enables **verbose mode** to display detailed scan results.

The scan detects **open TCP ports**, **running services**, and the **TTL value of 128**, indicating that the



Edit with WPS Office

target OS is likely Microsoft Windows (Windows 7/8/8.1/10 or Windows Server 2008/12/16).

- The command `unicornscan 10.10.1.9 -lv` is used to perform a detailed scan on the target machine, which in this case is Ubuntu (10.10.1.9).

```
[root@parrot]~
#unicornscan 10.10.1.16 -lv
adding 10.10.1.16/32 mode `TCPscan' ports `7,9,11,13,18,19,21-23,25,37,39,42,49,
50,53,65,67-70,79-81,88,98,100,105-107,109-111,113,118,119,123,129,135,137-139,1
43,150,161-164,174,177-179,191,199-202,204,206,209,210,213,220,345,346,347,369-3
72,389,406,407,422,443-445,487,500,512-514,517,518,520,525,533,538,548,554,563,5
37,610-612,631-634,636,642,653,655,657,666,706,750-752,765,779,808,873,901,923,9
41,946,992-995,1001,1023-1030,1080,1210,1214,1234,1241,1334,1349,1352,1423-1425,
1433,1434,1524,1525,1645,1646,1649,1701,1718,1719,1720,1723,1755,1812,1813,2048-
2050,2101-2104,2140,2150,2233,2323,2345,2401,2430,2431,2432,2433,2583,2628,2776,
2777,2988,2989,3050,3130,3150,3232,3306,3389,3456,3493,3542-3545,3632,3690,3801,
4000,4400,4321,4567,4899,5002,5136-5139,5150,5151,5222,5269,5308,5354,5355,5422-
5425,5432,5503,5555,5556,5678,6000-6007,6346,6347,6543,6544,6789,6838,6666-6670,
7000-7009,7028,7100,7983,8079-8082,8088,8787,8879,9090,9101-9103,9325,9359,10000
,10026,10027,10067,10080,10081,10167,10498,11201,15345,17001-17003,18753,20011,2
0012,21554,22273,26274,27374,27444,27573,31335-31338,31787,31789,31790,31791,326
58,32767-32780,33390,47262,49301,54320,54321,57341,58008,58009,58666,59211,60000
,60006,61000,61348,61466,61603,63485,63808,63809,64429,65000,65506,65530-65535'
ops 300
using interface(s) eth0
scanning 1.00e+00 total hosts with 3.38e+02 total packets, should take a little l
onger than 8 Seconds
```

The scan detects open TCP ports, running services, and a TTL value of 64, indicating that the target OS is likely Linux-based (Google Linux, Ubuntu, Parrot, or Kali).

```
TCP open 10.10.1.9:80  ttl 64
TCP open 10.10.1.9:22  ttl 64
sender statistics 295.5 pps with 338 packets sent total
listener statistics 676 packets received 0 packets dropped and 0 interface drops
TCP open [Attacks] ssh[ 22] from 10.10.1.9  ttl 64
TCP open [Attacks] http[ 80] from 10.10.1.9  ttl 64
```



Question 2.2.4.1

Run the Unicornscan tool from the Parrot Security machine to perform OS discovery on the target system (10.10.1.9). Enter YES if the target system is a Linux-based machine; else, enter NO.

yes

Score

✓ Correct

- Perform enumeration on a system or network to extract usernames, machine names, network resources, shares, etc.

Enumeration is the process of actively gathering detailed information about a target system by establishing a connection and performing queries. It helps in identifying usernames, user groups, shared folders, active services, open ports, OS type, machine name, and network configuration. Enumeration techniques are conducted in intranet environments to identify vulnerabilities for security analysis or exploitation.

■ Perform NetBIOS enumeration using Windows Command-Line utilities

- First switch to the Windows Server 2019 (10.10.1.19) machine and activate it using **Ctrl+Alt+Delete**. Log in with the **Administration** profile by pasting **Pa\$\$w0rd** in the password field. Alternatively, use the **Type Password** option under the **Commands** menu. When the **Networks** screen appears, click **Yes** to allow network discovery.
- Run the command:
 - **nbtstat -a 10.10.1.10**
 - This displays the NetBIOS name table of the remote **Windows 10** machine, revealing active NetBIOS names and their associated types.



Edit with WPS Office

```
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbtstat -a 10.10.1.10

Ethernet:
NodeIpAddress: [10.10.1.19] Scope Id: []

          NetBIOS Remote Machine Name Table

      Name           Type       Status
-----
WINDOWS10    <00>   UNIQUE   Registered
WORKGROUP    <00>   GROUP    Registered
WINDOWS10    <20>   UNIQUE   Registered
WORKGROUP    <1E>   GROUP    Registered
WORKGROUP    <1D>   UNIQUE   Registered
@MSBROWSE@<01> GROUP    Registered

MAC Address = 00-15-5D-01-80-01
```

■ NOW Run the command:

- **nbtstat -c**
- This lists the NetBIOS name cache, showing stored NetBIOS names and their resolved IP addresses without requiring authentication.

```
C:\Users\Administrator>nbtstat -c

Ethernet:
NodeIpAddress: [10.10.1.19] Scope Id: []

          NetBIOS Remote Cache Name Table

      Name           Type       Host Address     Life [sec]
-----
WINDOWS10    <20>   UNIQUE   10.10.1.10      351

C:\Users\Administrator>
```

■ Run the command:

- **net use**
- This displays active network connections, including shared folders, drives, and connection status.



Edit with WPS Office

```
C:\Users\Administrator>net use  
C:\  
New connections will be remembered.  
  
Status Local Remote Network  
---- -- -- --  
W:OK Z: \\WINDOWS10\EHE-Tools Microsoft Windows Network  
The command completed successfully.  
  
C:\Users\Administrator>
```

- 9. This concludes the demonstration of performing NetBIOS enumeration using Windows command-line utilities such as Nbtstat and Net use.
- 10. Close all open windows and document all the acquired information.

Question 2.3.1.1

Name the shared folder/drive available for the Windows Server 2019 machine.

\\\Windows10\EHE-Tools

Score

 Correct

■ Perform NetBIOS enumeration using NetBIOS Enumerator

NetBIOS Enumerator is a tool for gathering network details like NetBIOS names, usernames, domain names, and MAC addresses using SMB.

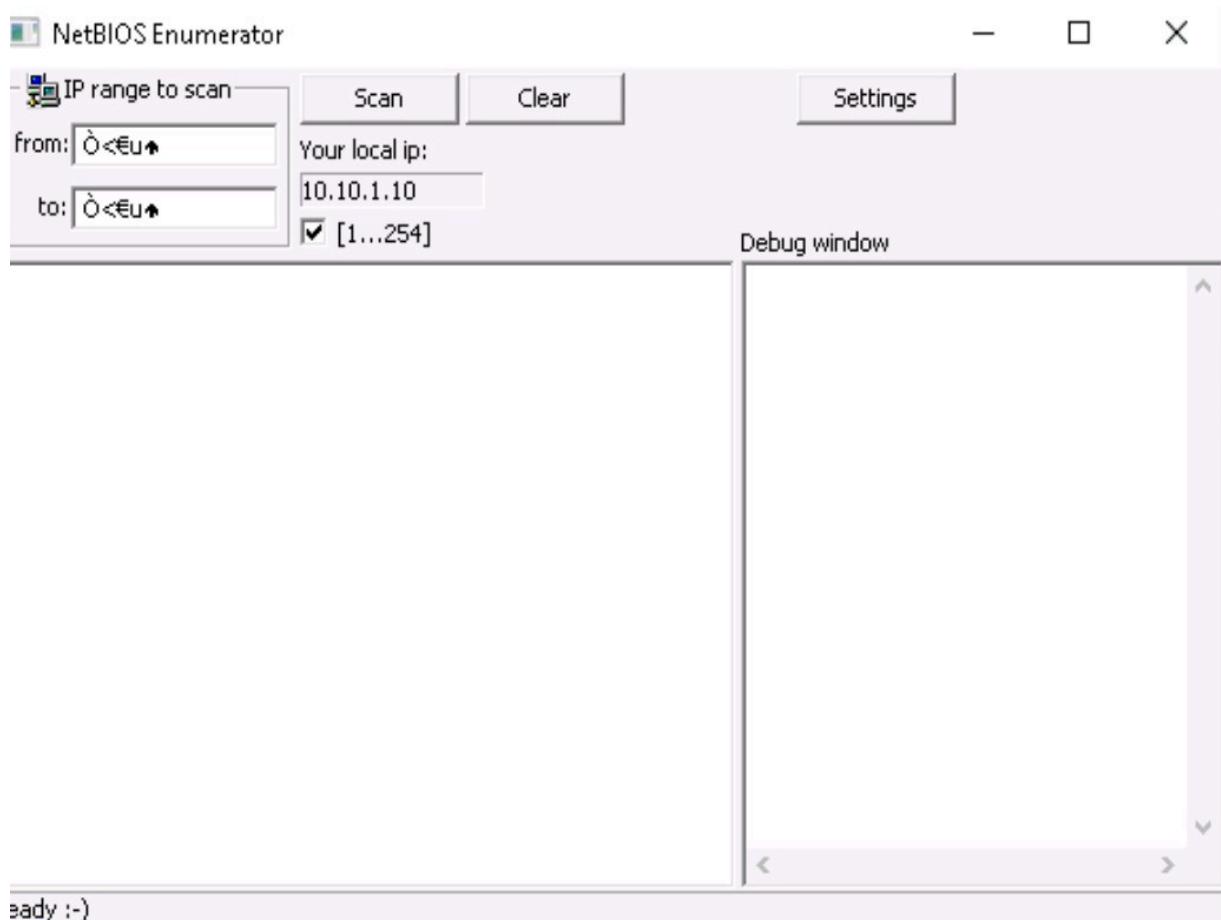
Here, a Windows 10 machine is used to perform NetBIOS enumeration on Windows Server 2016 and Windows Server 2019 machines.

- Switch to the Windows 10 machine.
- Navigate to D:\\EHE-Tools\\EHE Module 02 Ethical Hacking Fundamentals\\NetBIOS Enumeration Tools\\NetBIOS Enumerator and double-click NetBIOS Enumerator.exe.
- If a security warning appears, click Run. The NetBIOS Enumerator main window will open.

- The NetBIOS Enumerator main window appears, as shown in the screenshot.



Edit with WPS Office

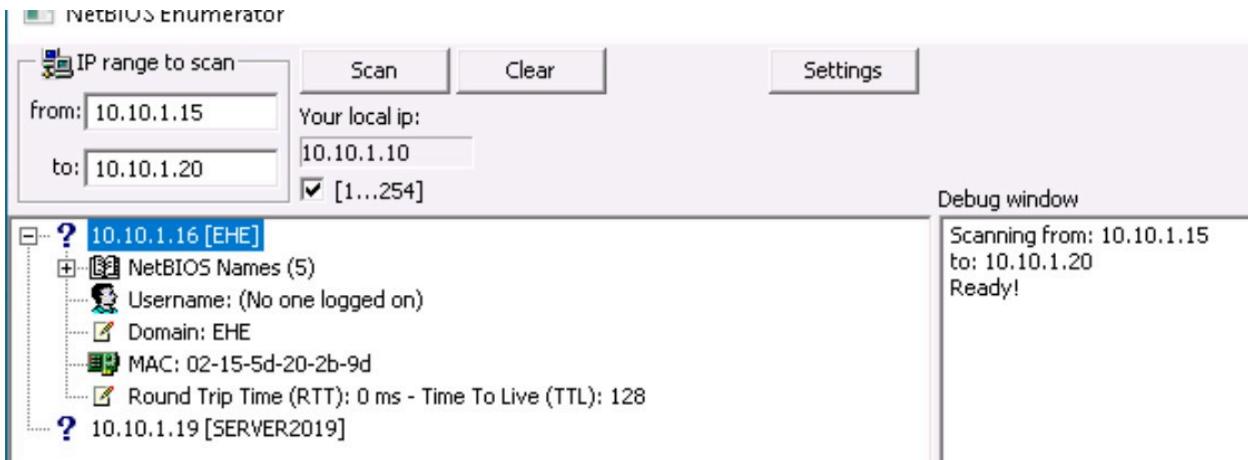


- Under **IP range to scan** put IP range **10.10.1.15-10.10.1.20** and click **scan**.
- NetBIOS Enumerator scans the specified IP address range. Once completed, the scan results appear in the left pane.
- The **Debug window** in the right pane shows the scanning progress and displays **Ready!** when the scan is finished.



Edit with WPS Office

- Click the expand icon (+) next to 10.10.1.16 and 10.10.1.19 in the left pane to reveal their details.
- Next, expand NetBIOS Names to view the NetBIOS details of the target IP addresses.



- 8. This concludes the demonstration of performing NetBIOS enumeration using NetBIOS Enumerator. This enumerated NetBIOS information can be used to strategize an attack on the target.
- 9. Close all open windows and document all the acquired information.

Question 2.3.2.1

Use the NetBIOS Enumerator tool to perform NetBIOS enumeration on the network (10.10.1.15 - 10.10.1.20). NetBIOS Enumerator tool is available at D:\EHE-Tools\EHE Module 02 Ethical Hacking Fundamentals\NetBIOS Enumeration Tools\NetBIOS Enumerator. Enter the domain name associated with the IP address 10.10.1.16.

EHE

Score

Correct

Ethical Hacking Lab Report – 06 (Date: 12-05-2025)

EC-Council Lab Assignment: Module 3

Information Security Threats and Vulnerability Assessment

Scenario

A threat is a possible event that can harm or disrupt an organization's operations. Threats can be physical or digital, and may be accidental, intentional, or due to other causes. Cyber threats often target personal, financial, and login data, and compromised systems may be used for further malicious actions. The severity of a threat depends on its potential damage, detection difficulty, and control level. Threats can compromise the



Edit with WPS Office

Confidentiality, Integrity, and Availability (CIA) of data, causing data loss, identity theft, and other cybercrimes.

In this module's labs, you'll explore how attackers create and spread malware, and how to assess vulnerabilities in systems and networks.

Objective

This lab helps you:

- Create and deploy a Trojan to exploit a target system
- Develop a virus to infect a target machine
- Perform vulnerability assessments to find system/network weaknesses

Overview of Threats

Types of Threats:

- Natural Threats: Disasters like floods, fires, earthquakes, and power failures that can damage IT infrastructure.
 - Unintentional Threats: Human errors, poor training, or negligence within an organization.
 - Intentional Threats:
 - Internal: Insider threats by employees with access to systems
 - External: Attackers exploiting system vulnerabilities from outside
- [Lab 1: Create a Trojan to Gain Access to the Target System](#)

Scenario

A Trojan disguises itself as a legitimate program but secretly performs harmful actions. Attackers may use it to control systems remotely, steal data, or launch other attacks. Systems using unencrypted credentials are especially vulnerable. Trojans can enter via email, downloads, or instant messaging and may spoof their origin to mislead investigations.

This lab shows how attackers take control of systems using Trojans and establish hidden channels for data transfer.

Objectives



Edit with WPS Office

- Create a Trojan Server with Theef RAT
- Control a Victim System using njRAT

Task 1: Create a Trojan Server using Theef RAT Trojan

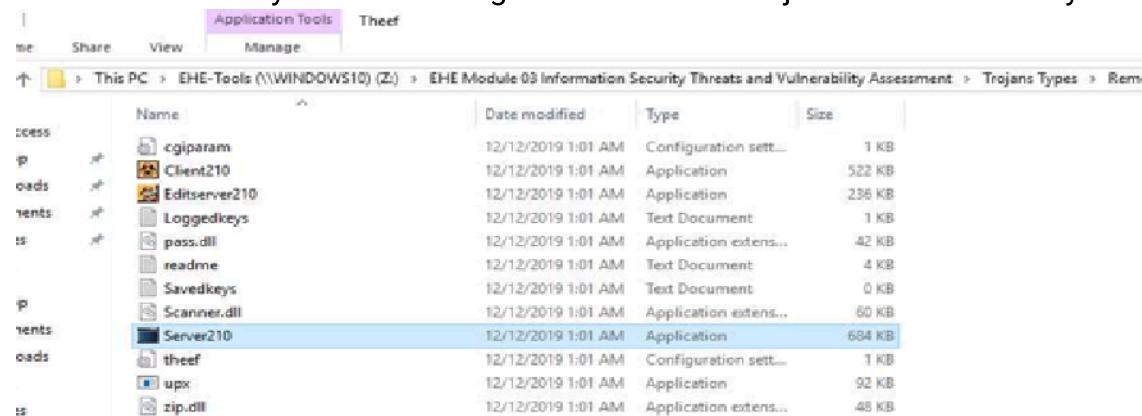
Remote Access Trojans (RATs) let attackers gain full remote control of a system, including screen and webcam access, file management, keylogging, and command execution. These RATs spread via phishing, USB drives, or drive-by downloads.

Theef RAT, written in Delphi, operates over port 9871 and consists of a client (attacker's control panel) and server (malicious file installed on the victim's system). Though interface versions may differ, the creation process remains consistent

In this lab, for demonstration purposes, we are directly executing the file on the victim machine, Windows Server 2016. And Windows 10 machine (as an attacker)

On the Victim's Machine (Windows Server 2016)

1. Navigate to:
Z:\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\Theef
2. Run Server210.exe by double-clicking it to initiate the Trojan on the victim's system.



On the Attacker's Machine (Windows 10)

1. Navigate to:
D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\Theef
2. Launch Client210.exe to open the attack interface.
3. Enter the IP address of the victim machine.
4. A remote session is successfully established with the Windows Server 2016



Edit with WPS Office

system

The screenshot shows a Windows File Explorer window with the following details:

Path: This PC > EHE-Tools (\Windows10) (Z:) > EHE Module 03 Information Security Threats and Vulnerability Assessment > Trojans Types > Remote Access Trojans (RAT) > Theef

| Name | Date modified | Type | Size |
|---------------|--------------------|-----------------------|--------|
| cgiparam | 12/12/2019 1:01 AM | Configuration sett... | 1 KB |
| Client210 | 12/12/2019 1:01 AM | Application | 522 KB |
| Editserver210 | 12/12/2019 1:01 AM | Application | 236 KB |
| Loggedkeys | 12/12/2019 1:01 AM | Text Document | 1 KB |
| pass.dll | 12/12/2019 1:01 AM | Application exten... | 42 KB |
| readme | 12/12/2019 1:01 AM | Text Document | 4 KB |
| Savedkeys | 12/12/2019 1:01 AM | Text Document | 0 KB |
| Scanner.dll | 12/12/2019 1:01 AM | Application exten... | 60 KB |
| Server210 | 12/12/2019 1:01 AM | Application | 684 KB |
| theef | 12/12/2019 1:01 AM | Configuration sett... | 1 KB |
| upx | 12/12/2019 1:01 AM | Application | 92 KB |
| zip.dll | 12/12/2019 1:01 AM | Application exten... | 48 KB |

In Attackers machine

Navigate to D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\Theef and double-click Client210.exe to access the victim machine remotely.

The screenshot shows a Windows File Explorer window with the following details:

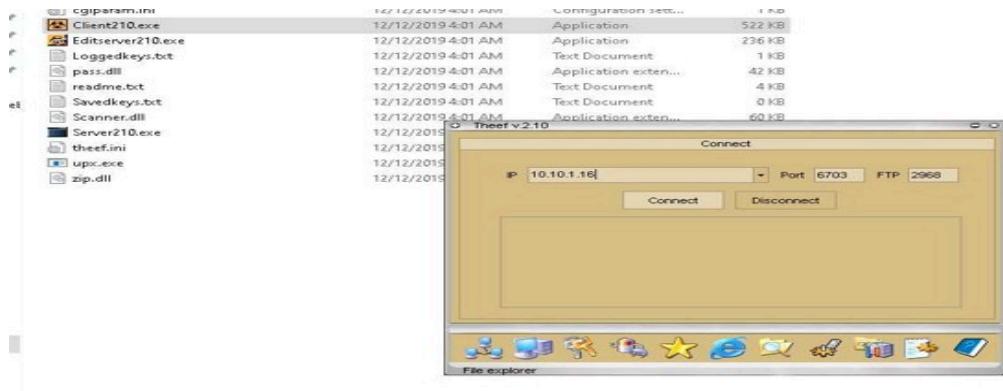
Path: This PC > EHE-Tools (D:) > EHE-Tools > EHE Module 03 Information Security Threats and Vulnerability Assessment > Trojans Types > Remote Acc

| Name | Date modified | Type | Size |
|-------------------|--------------------|-----------------------|--------|
| cgiparam.ini | 12/12/2019 4:01 AM | Configuration sett... | 1 KB |
| Client210.exe | 12/12/2019 4:01 AM | Application | 522 KB |
| Editserver210.exe | 12/12/2019 4:01 AM | Application | 236 KB |
| Loggedkeys.txt | 12/12/2019 4:01 AM | Text Document | 1 KB |
| pass.dll | 12/12/2019 4:01 AM | Application exten... | 42 KB |
| readme.txt | 12/12/2019 4:01 AM | Text Document | 4 KB |
| Savedkeys.txt | 12/12/2019 4:01 AM | Text Document | 0 KB |
| Scanner.dll | 12/12/2019 4:01 AM | Application exten... | 60 KB |
| Server210.exe | 12/12/2019 4:01 AM | Application | 684 KB |
| theef.ini | 12/12/2019 4:01 AM | Configuration sett... | 1 KB |
| upx.exe | 12/12/2019 4:01 AM | Application | 92 KB |
| zip.dll | 12/12/2019 4:01 AM | Application exten... | 48 KB |

Enter the IP address of the victim's system.



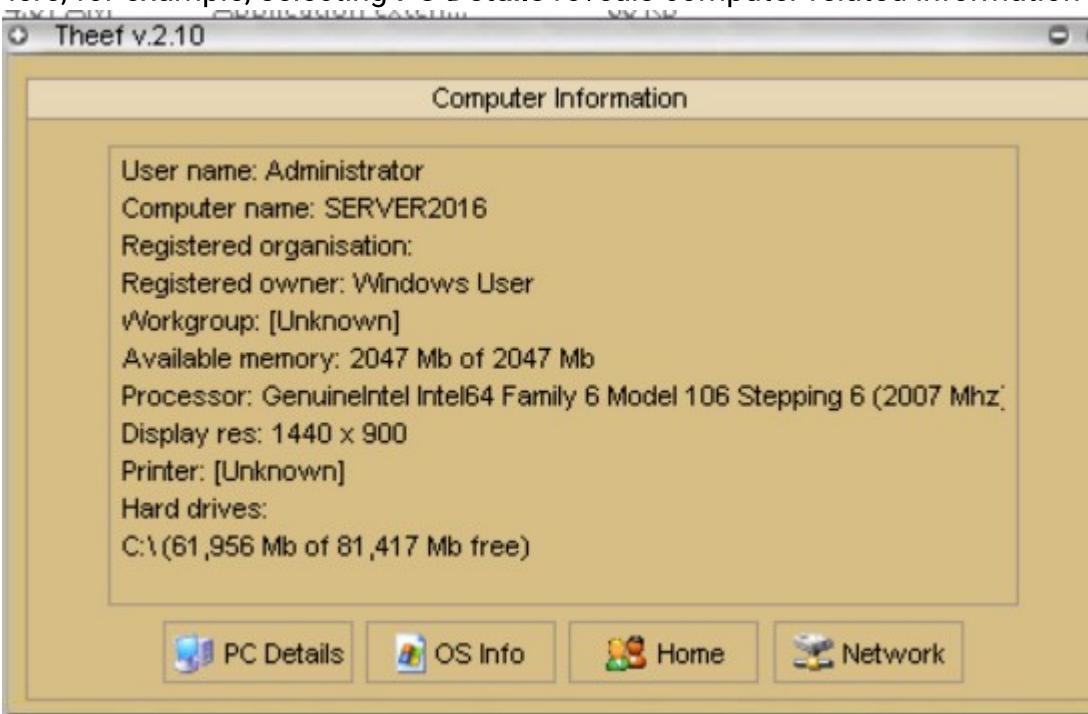
Edit with WPS Office



From **Windows 10**, we have successfully established a remote connection with the **Windows Server 2016** machine.

1. In **Computer Information**, we can view **PC Details**, **OS Info**, **Home**, and **Network** by clicking their respective buttons.

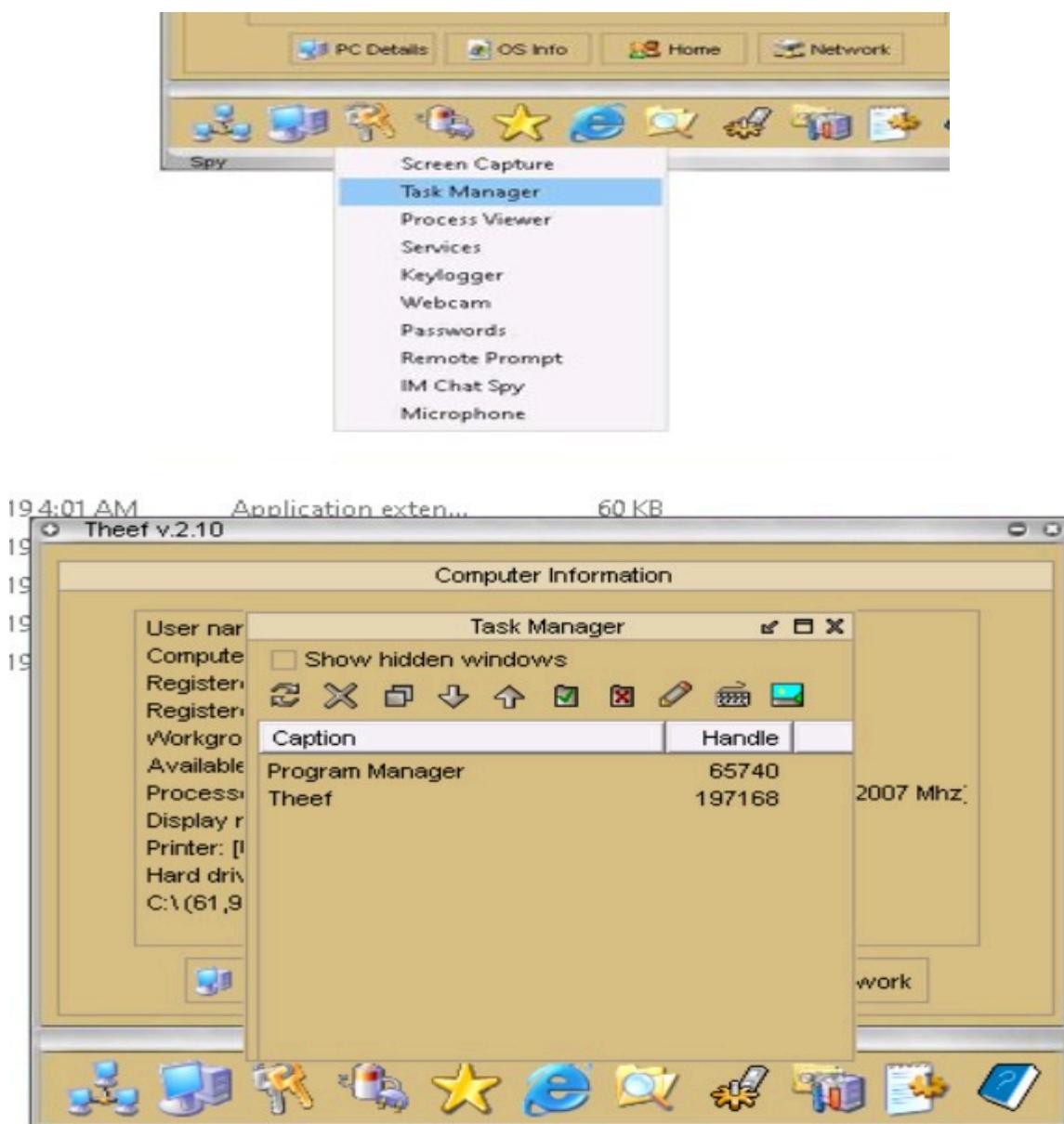
Here, for example, selecting **PC Details** reveals computer-related information



Spy icon to perform various operations like capture screens, log keys, view processes, view the task manager, use the webcam, and use the microphone on the target machine



For instance, selecting **Task Manager** views the tasks running on the target machine



Similarly For capturing keylogger event of the victim computer. Attacker's System



Edit with WPS Office



Question 3.1.1.1

Use the Windows 10 machine (10.10.1.10) as the attacker machine and Windows Server 2016 machine (10.10.1.16) as the victim machine. Create a trojan server using the Theef RAT trojan to control the victim machine remotely. Run the Theef server on the victim machine and Theef client on the attacker machine. The Theef client and server files are available in the directory Z:\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\Theef on the attacker machine. What is the default port used in Theef?

6703

Score

✓ Correct

Task 2: Gain Control over a Victim Machine using the njRAT RAT Trojan

njRAT is a Remote Access Trojan (RAT) with advanced data-stealing features. It can log keystrokes, access the victim's camera, steal credentials stored in browsers, upload and download files, manipulate processes and files, and view the victim's desktop.

This RAT also allows attackers to control Botnets (networks of compromised computers), enabling them to update, uninstall, disconnect, restart, and terminate the



Edit with WPS Office

RAT, as well as rename its campaign ID. Additionally, it can be configured to spread through USB drives using the Command and Control server software.

In this lab exercise, we will use **njRAT** to take control of a victim machine. The **attacker machine** will be a Windows 10 machine (IP: 10.10.1.10), and the **victim machine** will be a Windows Server 2016 (IP: 10.10.1.16).

To begin, on the **Windows 10 machine**, navigate to:

D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\njRAT and double-click on njRAT v0.7d.exe.

| This PC > EHE-Tools (D:) > EHE-Tools > EHE Module 03 Information Security Threats and Vulnerability Assessment > Trojans Types > Remote Access | | | |
|--|---------------------------|----------------------|-----------------|
| Name | Date modified | Type | Size |
| nj_users | 8/9/2014 3:22 AM | File folder | |
| Plugin | 4/19/2021 12:55 AM | File folder | |
| I.contact | 12/12/2019 4:01 AM | Contact file | 0 KB |
| I.DAT | 12/12/2019 4:01 AM | DAT File | 0 KB |
| I.exe | 12/12/2019 4:01 AM | Application | 0 KB |
| GeoIP.dat | 12/12/2019 4:01 AM | DAT File | 1,267 KB |
| njRAT v0.7d.exe | 12/12/2019 4:01 AM | Application | 1,684 KB |
| stub.il | 12/12/2019 4:01 AM | IL File | 229 KB |
| Stub.manifest | 12/12/2019 4:01 AM | MANIFEST File | 1 KB |
| WinMM.Net.dll | 12/12/2019 4:01 AM | Application exten... | 43 KB |

njRAT is a Remote Access Trojan that enables automatic reconnection and provides a wide range of spying and control functionalities.

Steps to Configure njRAT:

1. Launch njRAT:

Open the njRAT GUI. A pop-up appears asking for the port number.

2. Set Port Number:

Enter the desired port – **5552** is used in this lab – and click **Start**.

3. Configure Server Using Builder:

- o Click the **Builder** button (bottom-left of the njRAT interface).

- o In the **Builder** dialog:

- **Host:** Enter the IP address of the attacker's machine – 10.10.1.10.



Edit with WPS Office

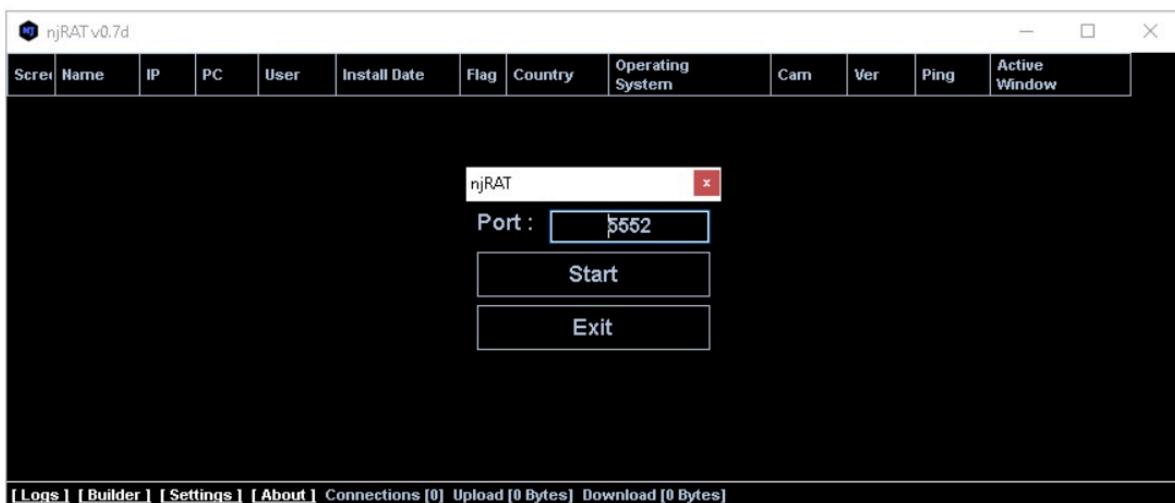
- **Enable:** Check the **Registry Startup** option.
- Leave other settings as default.
- Click **Build**.

4. Save the Server File:

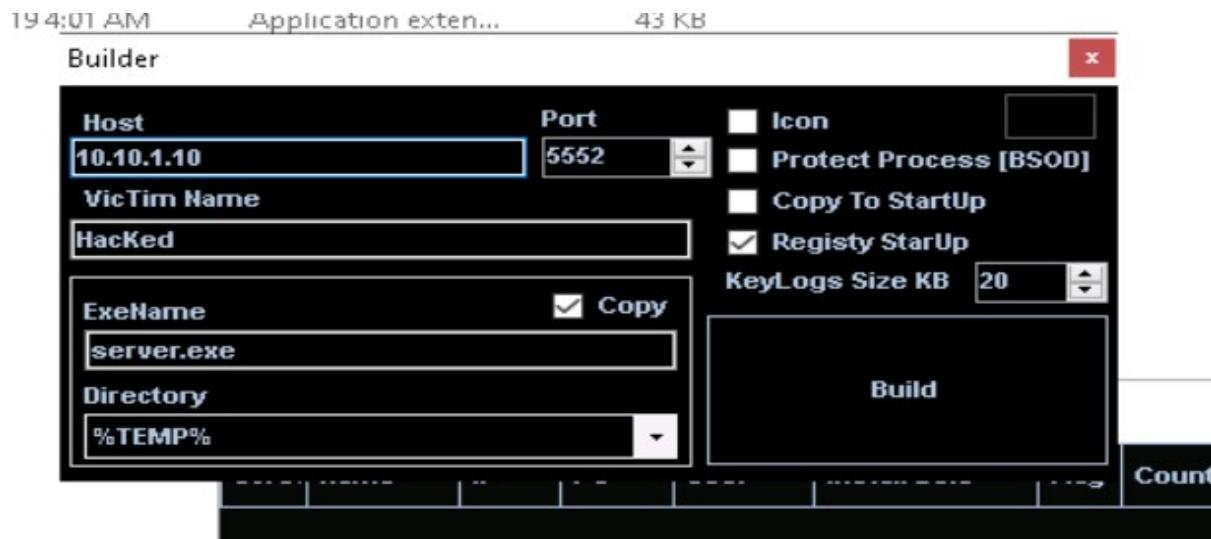
- o When prompted with the **Save As** dialog:
 - Save the file to the **Desktop**.
 - Name it **Test.exe**.
 - Click **Save**.

5. Build Confirmation:

After successful creation, a "DONE!" message appears. Click **OK** to finish



Edit with WPS Office



Switch to Windows server 2016 and Navigate to the shared network location (EHE-Tools), and then Copy and Paste the executable file (Test.exe) onto the Desktop of Windows Server 2016.

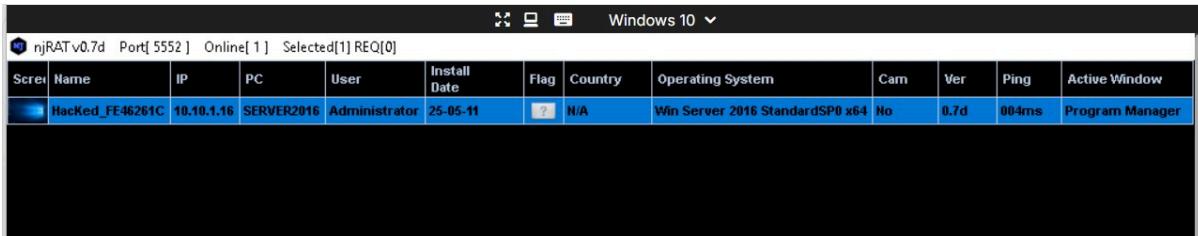


Double-click the server (Test.exe) to run this malicious executable

Click Windows 10 to switch back to the Windows 10 machine. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in Windows 10 establishes a persistent connection with the victim machine, as shown in the screenshot



Edit with WPS Office



The screenshot shows the njRAT v0.7d interface running on Windows 10. The title bar indicates "njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]". Below the title bar is a table with the following data:

| Screen | Name | IP | PC | User | Install Date | Flag | Country | Operating System | Cam | Ver | Ping | Active Window |
|--------|-----------------|------------|------------|---------------|--------------|------|---------|---------------------------------|-----|------|-------|-----------------|
| | Hacked_FE46261C | 10.10.1.16 | SERVER2016 | Administrator | 25-05-11 | ? | N/A | Win Server 2016 StandardSP0 x64 | No | 0.7d | 004ms | Program Manager |

Once a connection is established, njRAT GUI displays key details about the compromised system, including:

- IP Address
- Username
- Operating System

Steps to Control the Victim System:

1. Access Control Options:

- o Right-click on the victim machine listed in the njRAT interface.
- o Select **Manager** from the context menu.

2. File Manager Tab:

- o Opens by default in the Manager window.
- o Double-click any folder on the left panel (e.g., ProgramData) to browse its contents in the right panel.
- o Right-click on any file or folder to see options like Open, Delete, Rename, or Execute.

3. Process Manager Tab:

- o Click the **Process Manager** tab to view all running processes.
- o Right-click on any process to:
 - Kill (terminate),
 - Delete, or
 - Restart it



Edit with WPS Office



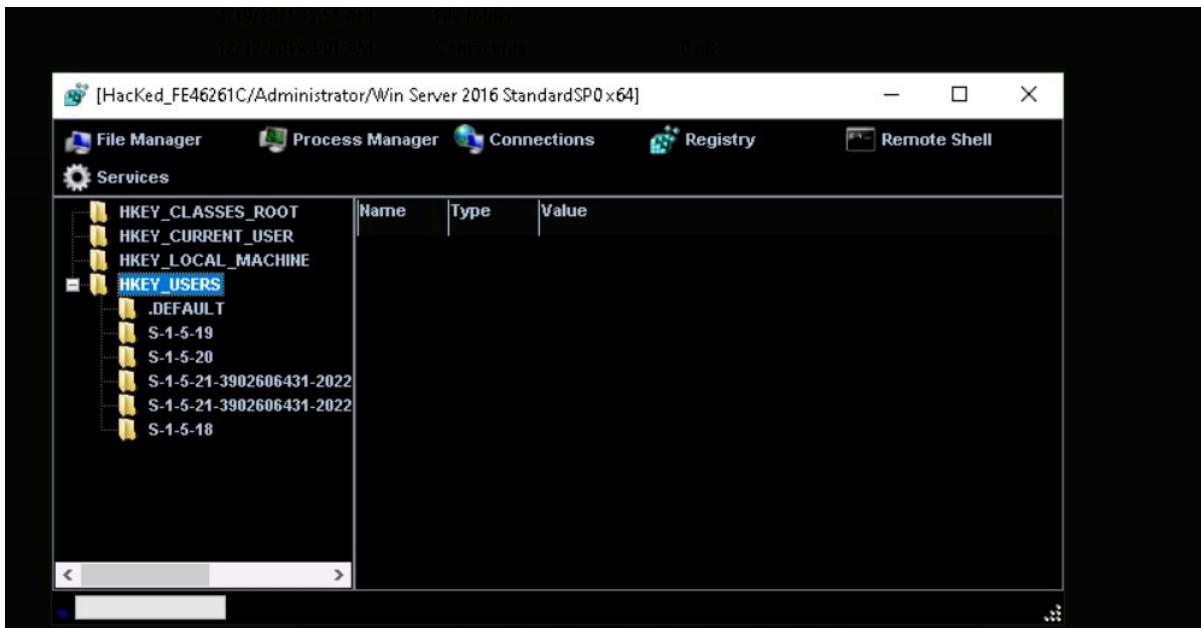
| | | | | |
|-------------------------|----------------|---|--------------------------|---|
| mqsvc.exe | 2948 | system32 | NETWORK SERVICE | |
| msdtc.exe | 3004 | System32 | NETWORK SERVICE | |
| nfsnt.exe | 2268 | system32 | NETWORK SERVICE | |
| RuntimeBroker.exe | 908 | System32 | Administrator | -Embedding |
| SearchUI.exe | 4476 | Microsoft.Windows.Cortana_cw5n1h2txyewy | Administrator | -ServerName:CortanaUI.AppXa50dqqa5gqv-428c9y1jjw7m3btvepj.mca |
| services.exe | 596 | Temp | Administrator | |
| services.exe | 596 | | SYSTEM | |
| ShellExperienceHost.exe | 4392 | ShellExperienceHost_cw5n1h2txyewy | Administrator | -ServerName:App.AppXtk18ttxbce2qsex02s8tw7hfxa9xb3t.mca |
| sihost.exe | 2192 | system32 | Administrator | |
| smss.exe | 288 | | SYSTEM | |
| SMSSvchost.exe | 2932 | v4.0.30319 | LOCAL SERVICE | |
| SMSSvchost.exe | 3296 | v4.0.30319 | NETWORK SERVICE | -NetMsmqActivator |
| snmp.exe | 2920 | System32 | SYSTEM | |
| spoolsv.exe | 2688 | System32 | SYSTEM | |
| svchost.exe | 780 | system32 | SYSTEM | -k DcomLaunch |
| svchost.exe | 836 | system32 | NETWORK SERVICE | -k RPCCS |
| svchost.exe | 936 | System32 | NETWORK SERVICE | -k termsvc |
| svchost.exe | 988 | System32 | LOCAL SERVICE | -k LocalServiceNetworkRestricted |
| svchost.exe | 996 | system32 | LOCAL SERVICE | -k LocalService |
| svchost.exe | 76 | System32 | SYSTEM | -k LocalSystemNetworkRestricted |
| svchost.exe | 392 | system32 | NETWORK SERVICE | -k NetworkService |
| svchost.exe | 800 | system32 | SYSTEM | -k ICSservice |

Finally, click on the **Connections** tab. After selecting a specific connection, right-click and choose **Kill Connection** to terminate the communication between the victim machine and the associated port

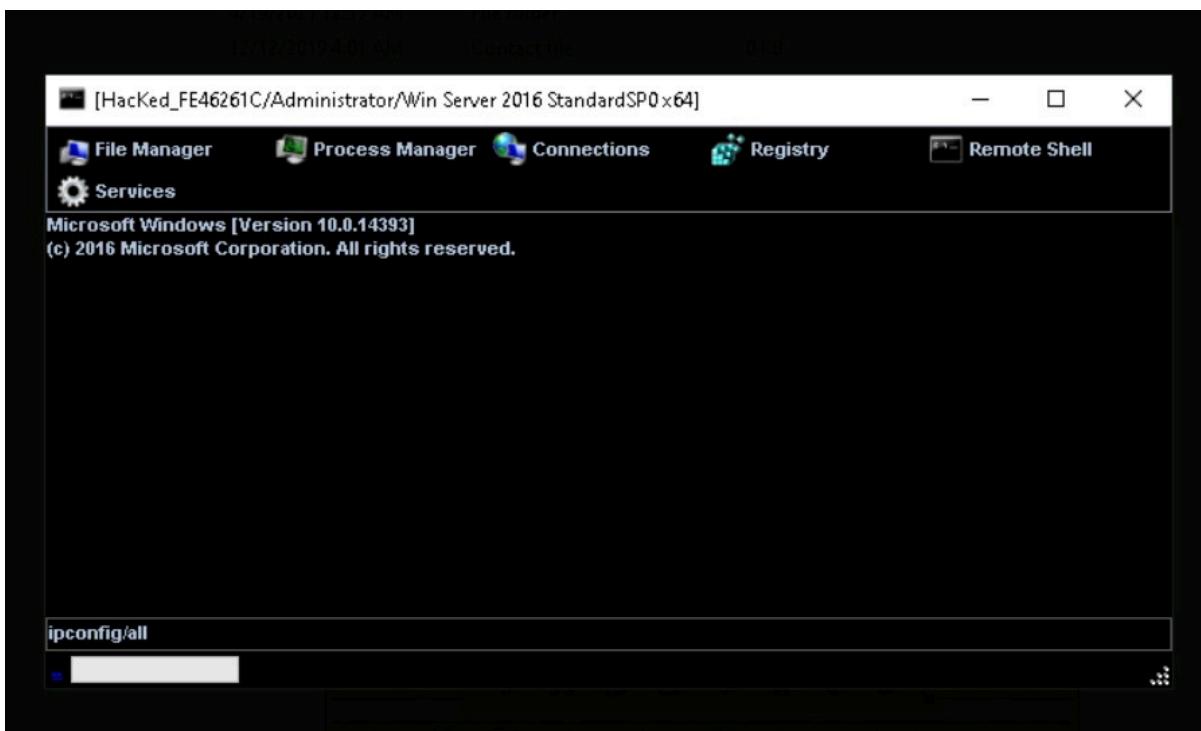
| | | | | | |
|------------|-------|---------|---|-----------------|---|
| 0.0.0.0 | 1545 | 0.0.0.0 | 0 | Listen | spoolsv[2948] |
| 0.0.0.0 | 1553 | 0.0.0.0 | 0 | Listen | services[596] |
| 0.0.0.0 | 1561 | 0.0.0.0 | 0 | Listen | dns[2912] |
| 0.0.0.0 | 1801 | 0.0.0.0 | 0 | Listen | mqsvc[2948] |
| 0.0.0.0 | 2103 | 0.0.0.0 | 0 | Listen | mqsvc[2948] |
| 0.0.0.0 | 2105 | 0.0.0.0 | 0 | Listen | mqsvc[2948] |
| 0.0.0.0 | 2107 | 0.0.0.0 | 0 | Listen | mqsvc[2948] |
| 0.0.0.0 | 2968 | 0.0.0.0 | 0 | Listen | dxreg[4888] |
| 0.0.0.0 | 3268 | 0.0.0.0 | 0 | Listen | lsass[604] |
| 0.0.0.0 | 3269 | 0.0.0.0 | 0 | Listen | lsass[604] |
| 0.0.0.0 | 3389 | 0.0.0.0 | 0 | Listen | svchost[936] |
| 0.0.0.0 | 5985 | 0.0.0.0 | 0 | Listen | System[4] |
| 0.0.0.0 | 6703 | 0.0.0.0 | 0 | Listen | dxreg[4888] |
| 0.0.0.0 | 9389 | 0.0.0.0 | 0 | Listen | Microsoft.ActiveDirectoryWebServices[2] |
| 0.0.0.0 | 47001 | 0.0.0.0 | 0 | Listen | System[4] |
| 10.10.1.16 | 53 | 0.0.0.0 | 0 | Listen | dnsc[2912] |
| 10.10.1.16 | 139 | 0.0.0.0 | 0 | Kill Connection | rem[4] |



Click the registry tab,

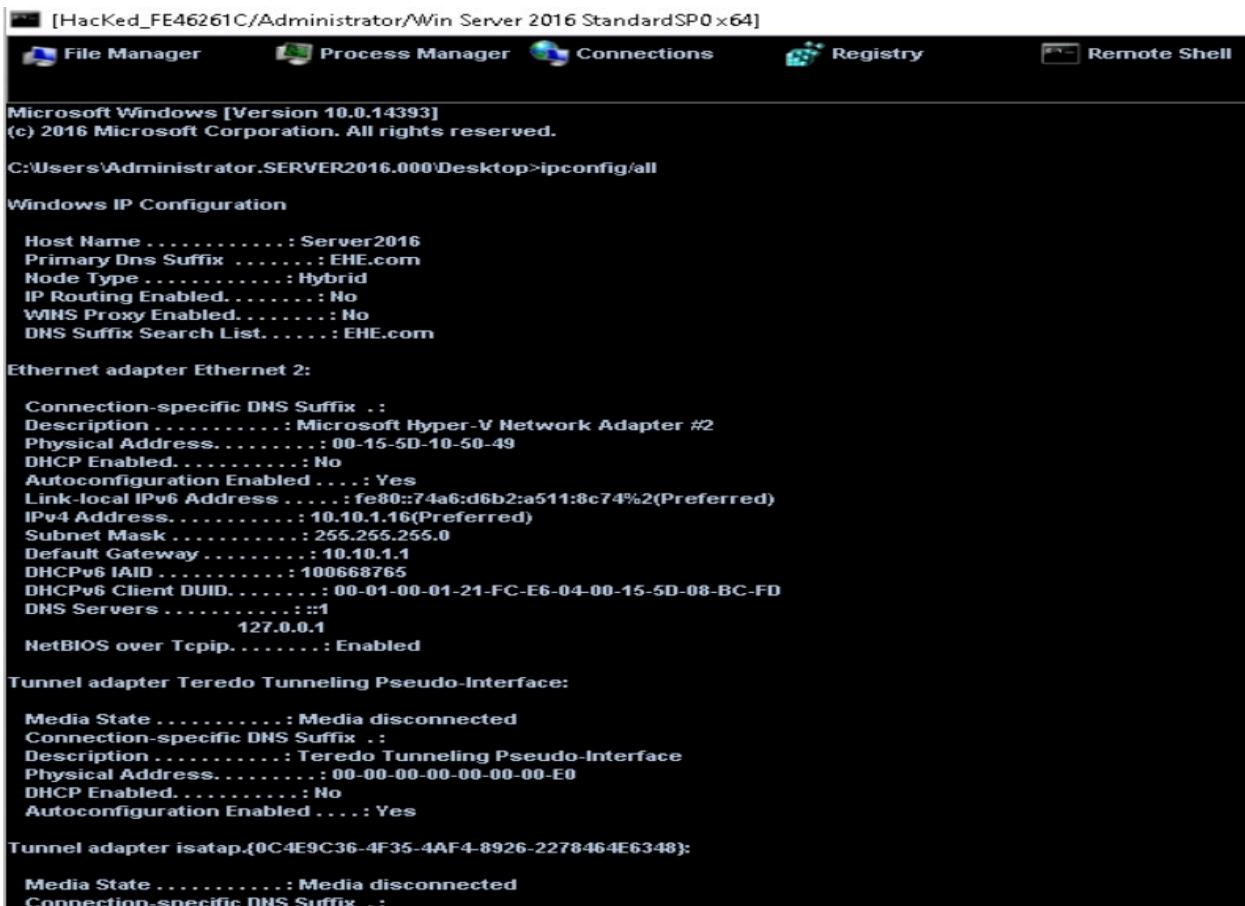


Click Remote Shell. This launches a remote command prompt for the victim machine Type the command ipconfig/all and press Enter.



Edit with WPS Office

This displays all interfaces related to the victim machine,



```
[HackEd_FE46261C\Administrator\Win Server 2016 Standard SP0 x64]
File Manager Process Manager Connections Registry Remote Shell

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.SERVER2016.000\Desktop>ipconfig/all

Windows IP Configuration

Host Name ..... : Server2016
Primary Dns Suffix ..... : EHE.com
Node Type ..... : Hybrid
IP Routing Enabled..... : No
WINS Proxy Enabled..... : No
DNS Suffix Search List..... : EHE.com

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix .:
Description ..... : Microsoft Hyper-V Network Adapter #2
Physical Address..... : 00-15-5D-10-50-49
DHCP Enabled..... : No
Autoconfiguration Enabled.... : Yes
Link-local IPv6 Address ..... : fe80::74a6:d6b2:a511:8c74%2(PREFERRED)
IPv4 Address..... : 10.10.1.16(Preferred)
Subnet Mask..... : 255.255.255.0
Default Gateway..... : 10.10.1.1
DHCPv6 IAID ..... : 100668765
DHCPv6 Client DUID..... : 00-01-00-01-21-FC-E6-04-00-15-5D-08-BC-FD
DNS Servers ..... ::1
127.0.0.1
NetBIOS over Tcpip..... : Enabled

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Media State ..... : Media disconnected
Connection-specific DNS Suffix .:
Description ..... : Teredo Tunneling Pseudo-Interface
Physical Address..... : 00-00-00-00-00-00-E0
DHCP Enabled..... : No
Autoconfiguration Enabled.... : Yes

Tunnel adapter isatap.{0C4E9C36-4F35-4AF4-8926-2278464E6348}:

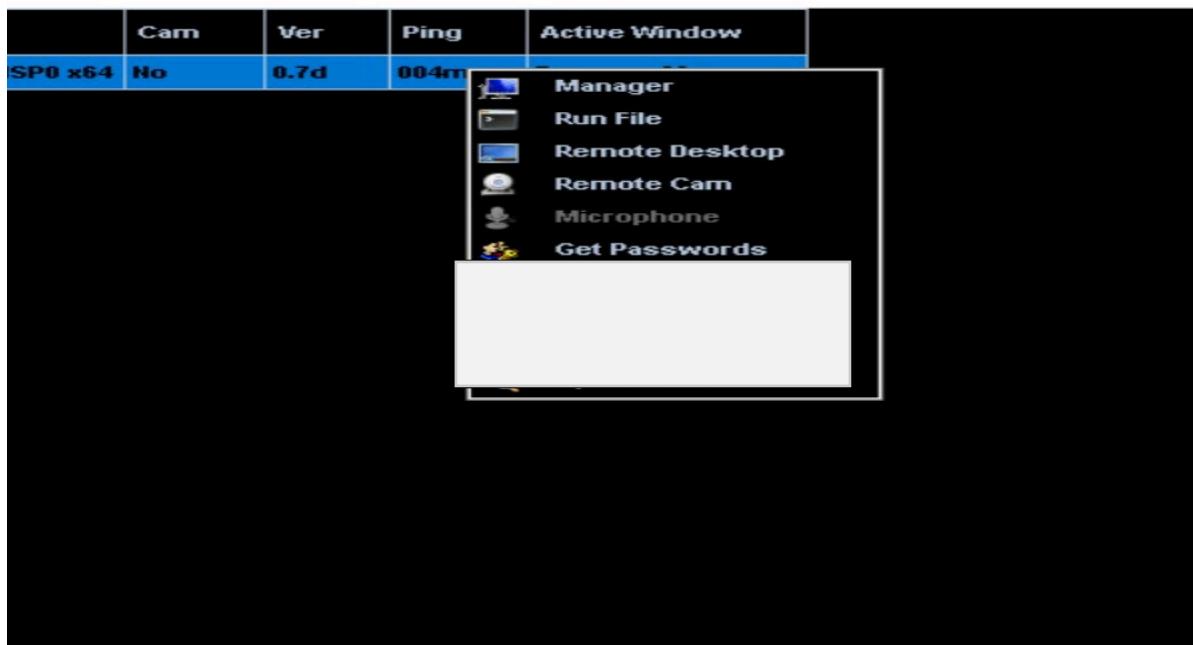
Media State ..... : Media disconnected
Connection-specific DNS Suffix .:
```

Now, Close the Manager window

Right-click on the victim name, and click Open Chat

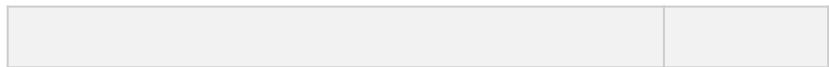


Edit with WPS Office

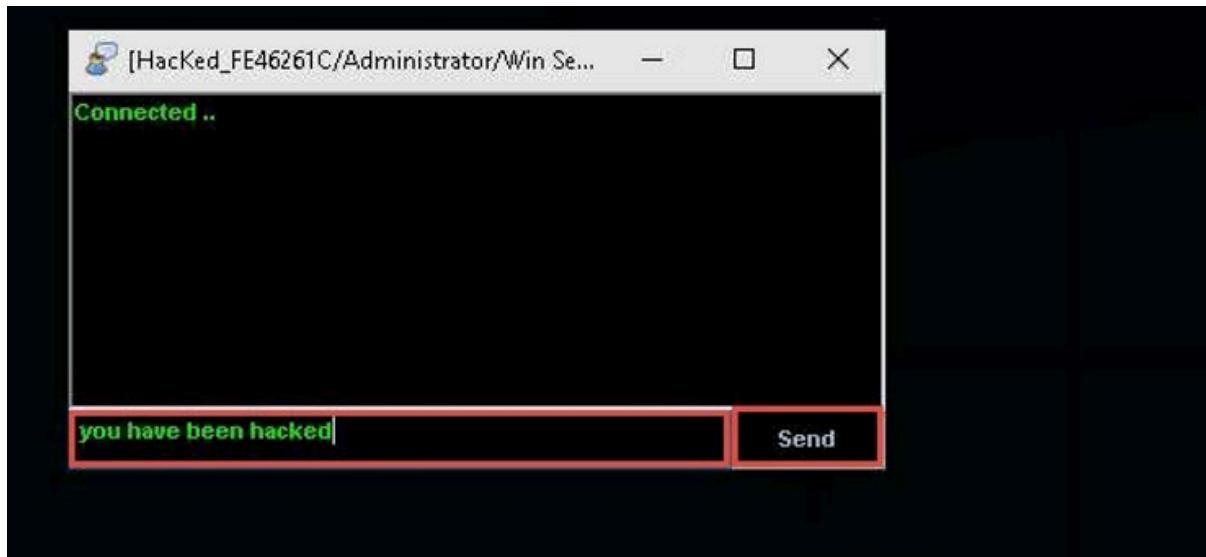


A Chat pop-up appears; enter a nickname (here, Hacker) and click OK

A chat box appears; type a message, and then click Send



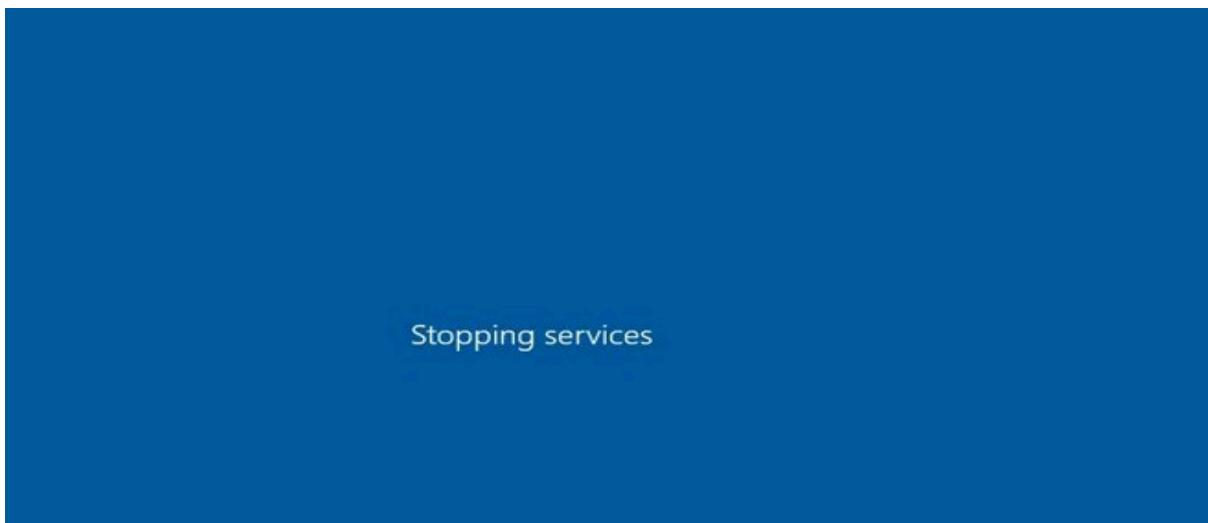
Edit with WPS Office



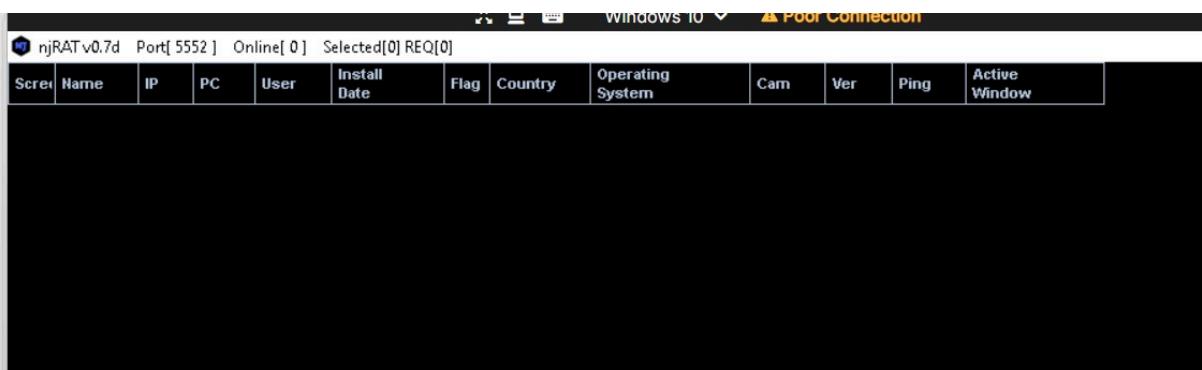
In Victim's Machine,



If the victim shut down the system , njRAT loses its connection with Windows Server 2016(victim)



Edit with WPS Office



njRAT is designed to automatically establish a connection once the victim logs in. After the malicious file is executed and the system restarts or the user logs back in, the **attacker's client (njRAT)** automatically detects and connects to the victim machine – no manual re-connection is needed



On completion of this lab, click [Windows Server 2016](#) to switch to the **Windows Server 2016** machine, launch **Task Manager**, look for the **server.exe (32 bit)** process



QUIZ:



Edit with WPS Office

Question 3.1.2.1

Use the Windows 10 machine (10.10.1.10) as the attacker machine and the Windows Server 2016 machine (10.10.1.16) as the victim machine. Run the njRAT trojan from the attacker machine at D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\njRAT and gain control over the victim machine. What is the primary DNS suffix of the victim machine?

EHE.com

Score

✓ Correct

Ethical Hacking Lab Report – 06 (Date: 05-05-2025)

EC-Council Lab Assignment: Module 4

Password Cracking Techniques and Countermeasures

Objective

- This lab is about understanding how passwords can be cracked. Password cracking means figuring out a password using different methods, like guessing or using special tools. People might crack passwords to recover their own lost passwords, check if a system is secure, or—unfortunately—break into systems without permission.
- In this lab, you will see how weaknesses in security can be exploited and how different password-cracking techniques work. The main goal is to learn how to monitor a system remotely and understand how someone might bypass security controls to gain access.
- It's important to use this knowledge responsibly—to strengthen security, not to break it! Let me know if you need a clearer explanation or more details.



Edit with WPS Office